SOPHOS

EVOLVE

Sophos EDR

Mit Forensik und Synchronized Security den Kampf gegen Emotet und Co. gewinnen

Anti-Virus gegen moderne Bedrohungen

Endpoint Technologien

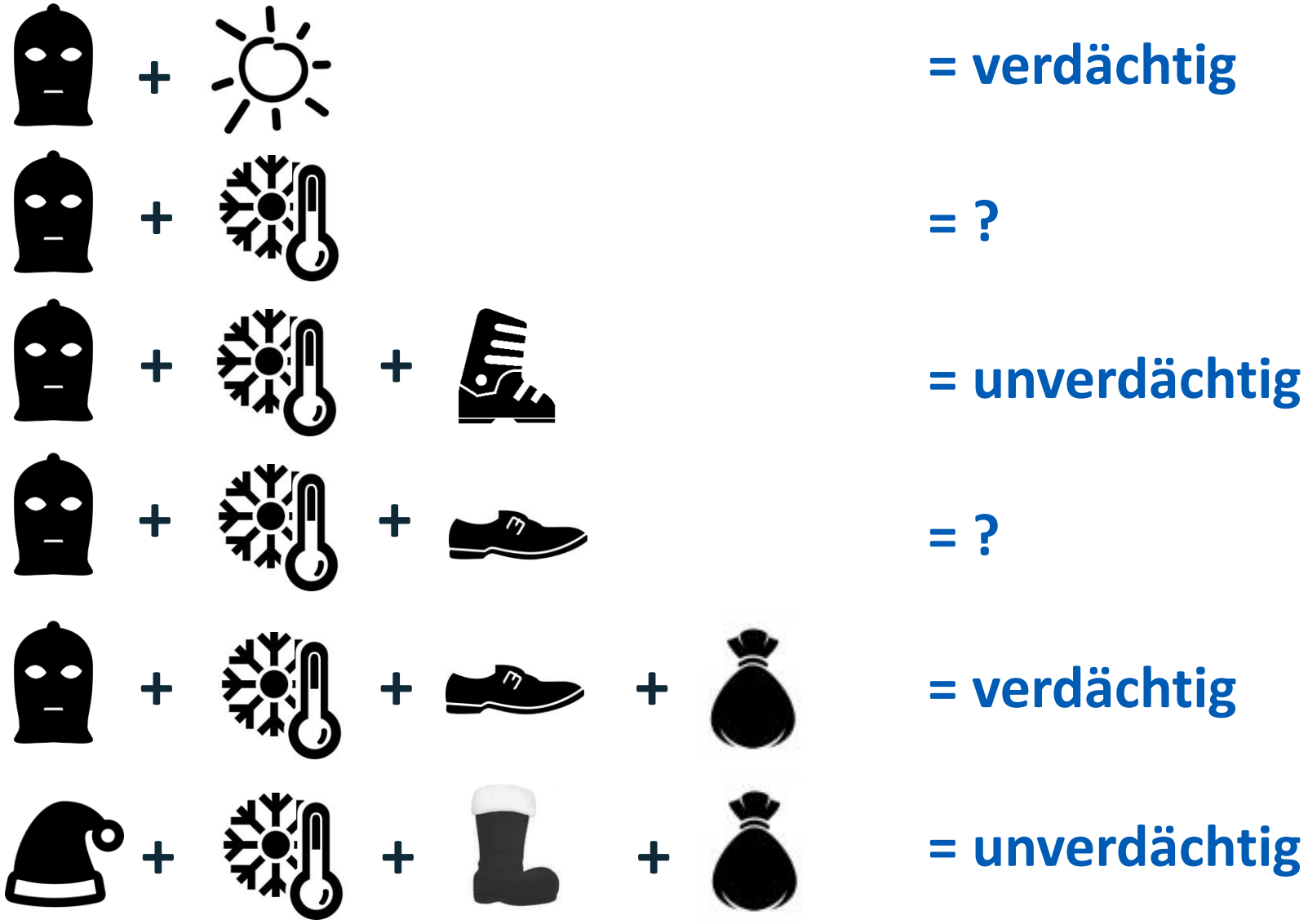
Bank

Anti-Virus

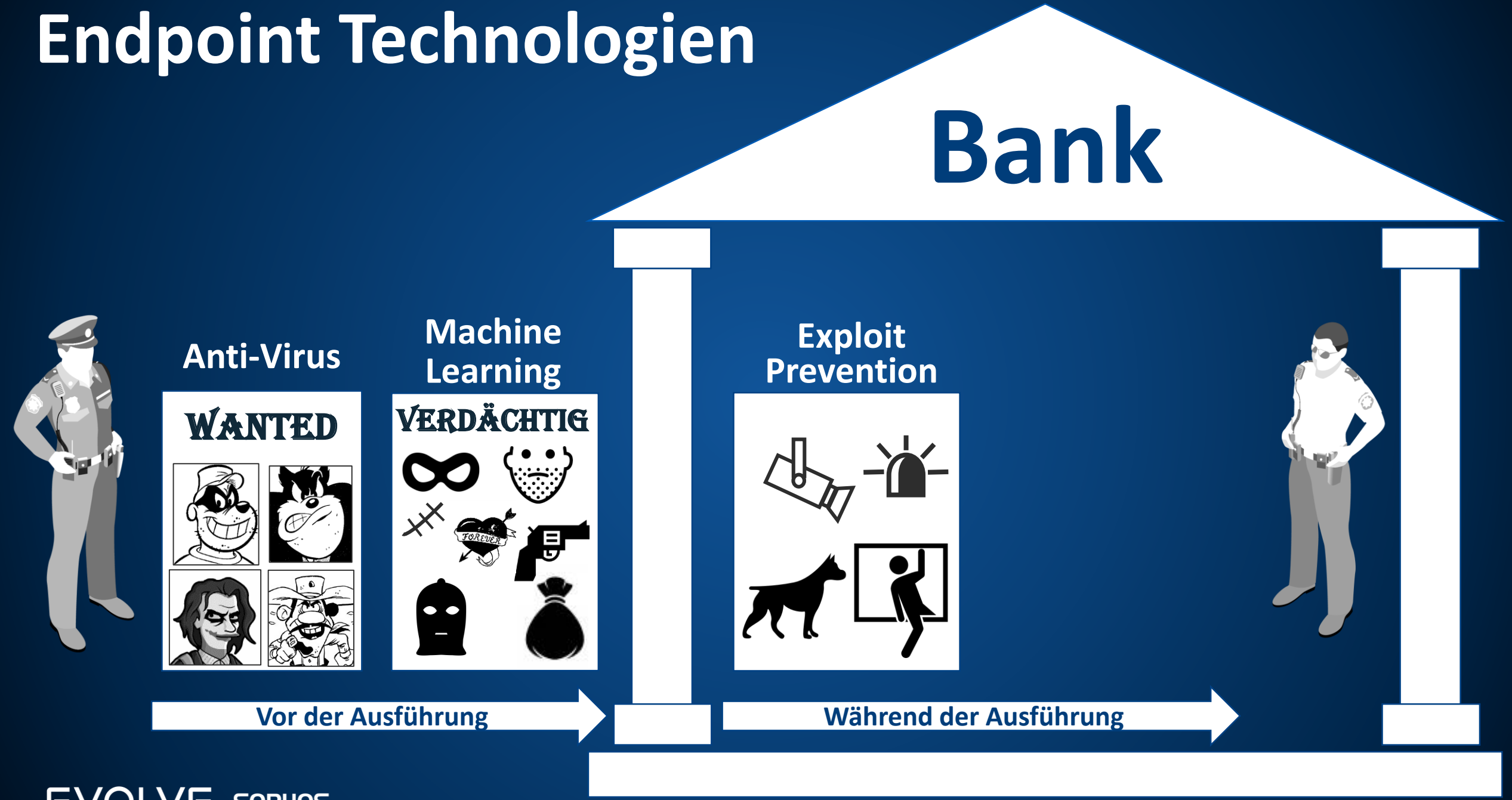
Machine Learning

Vor der Ausführung

Machine Learning



Endpoint Technologien



EVOLVE SOPHOS

Endpoint Technologien

Bank

Anti-Virus

Machine Learning

Exploit Prevention

Verhaltens-erkennung

Vor der Ausführung

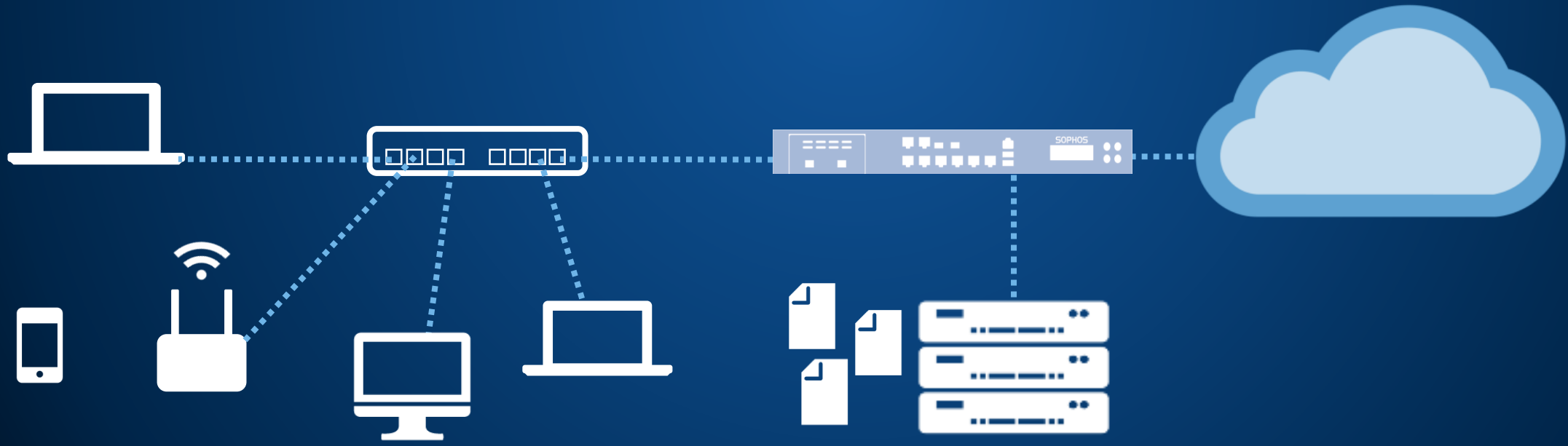
Während der Ausführung

EVOLVE SOPHOS

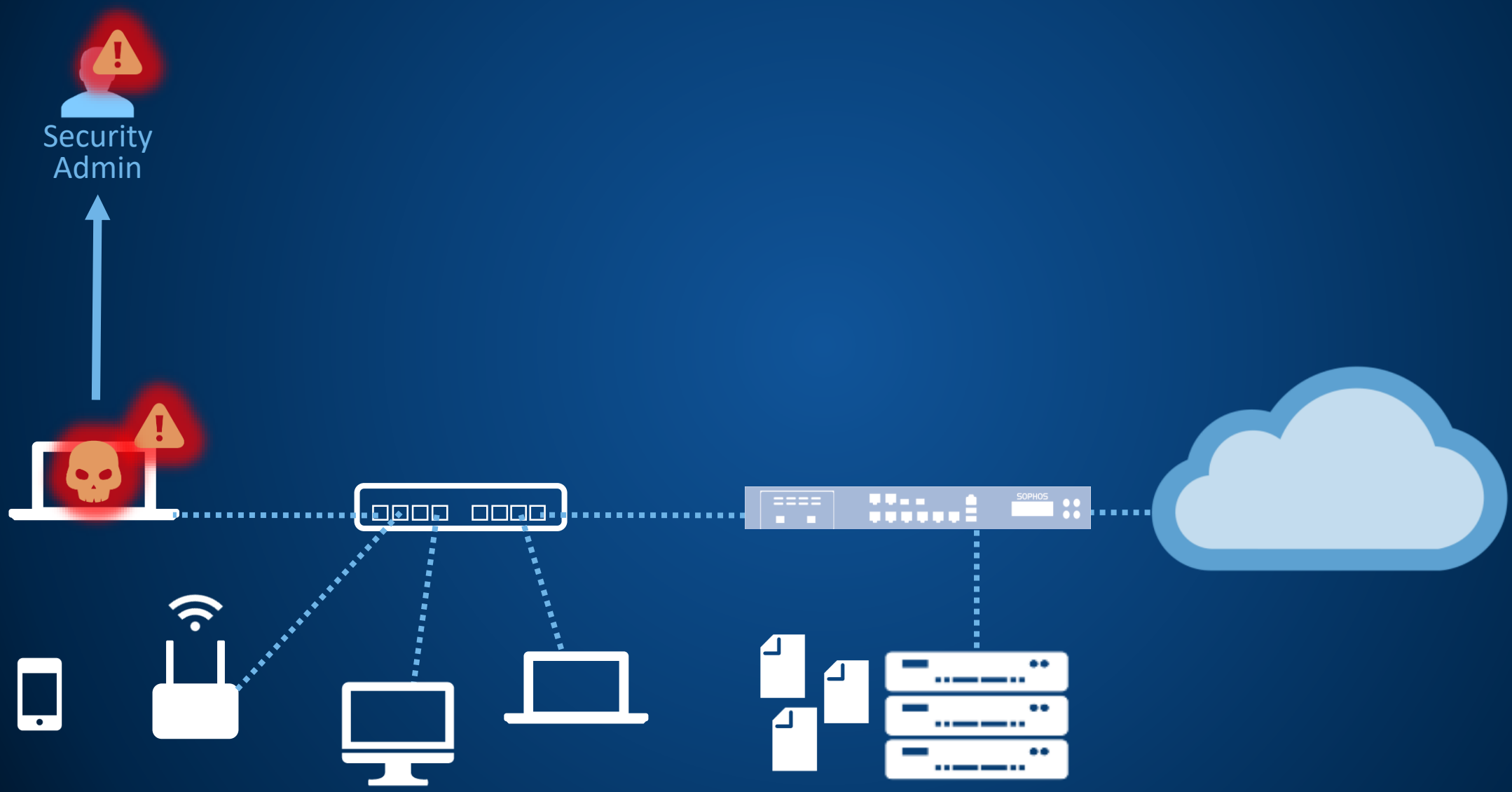
Und wie sieht das in der Praxis aus?

Neulich in Detroit…das Problem

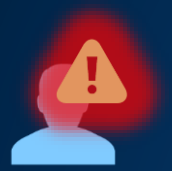
Am Beispiel einer Bedrohung



Die Bedrohung wird erkannt

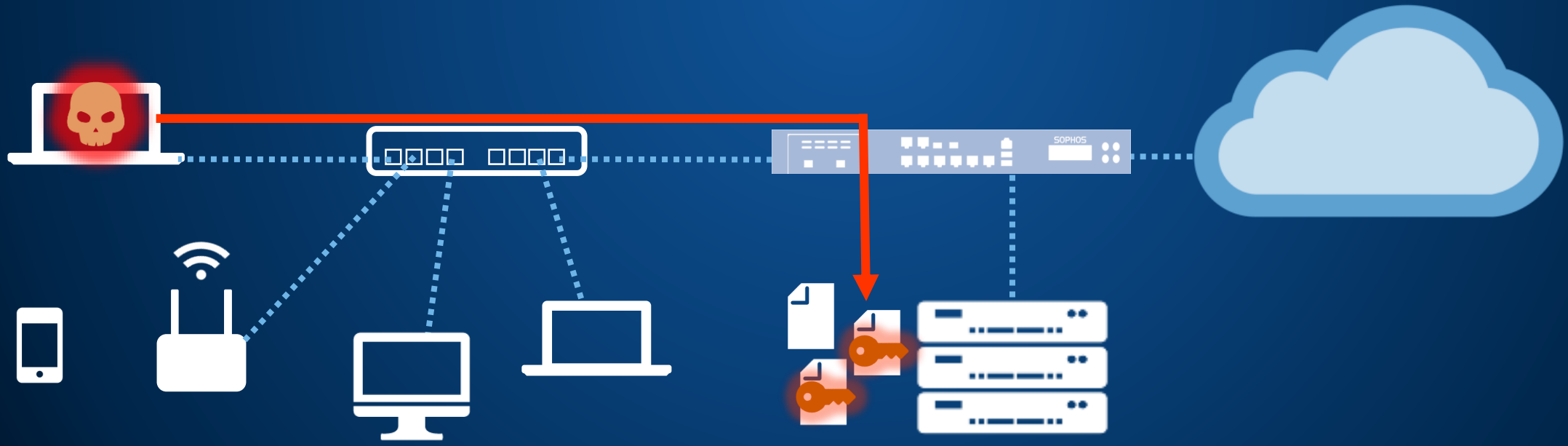


..und analysiert



Security Admin

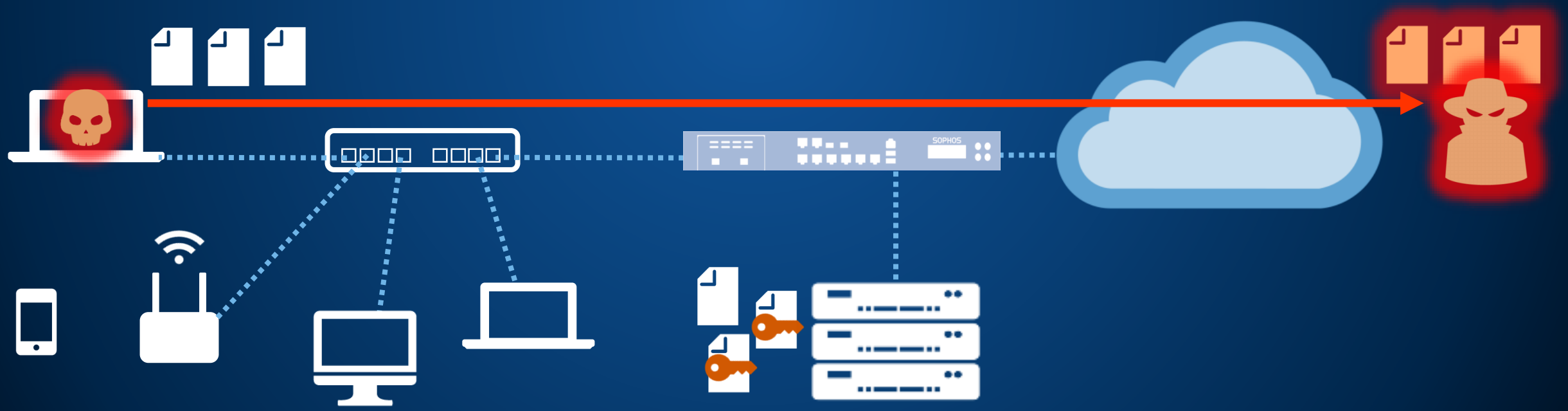
Es wurden Dateien auf dem Fileserver verschlüsselt



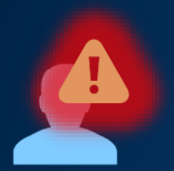
..und analysiert

Security Admin

..und vertrauliche Daten an einen Angreifer im Internet geschickt

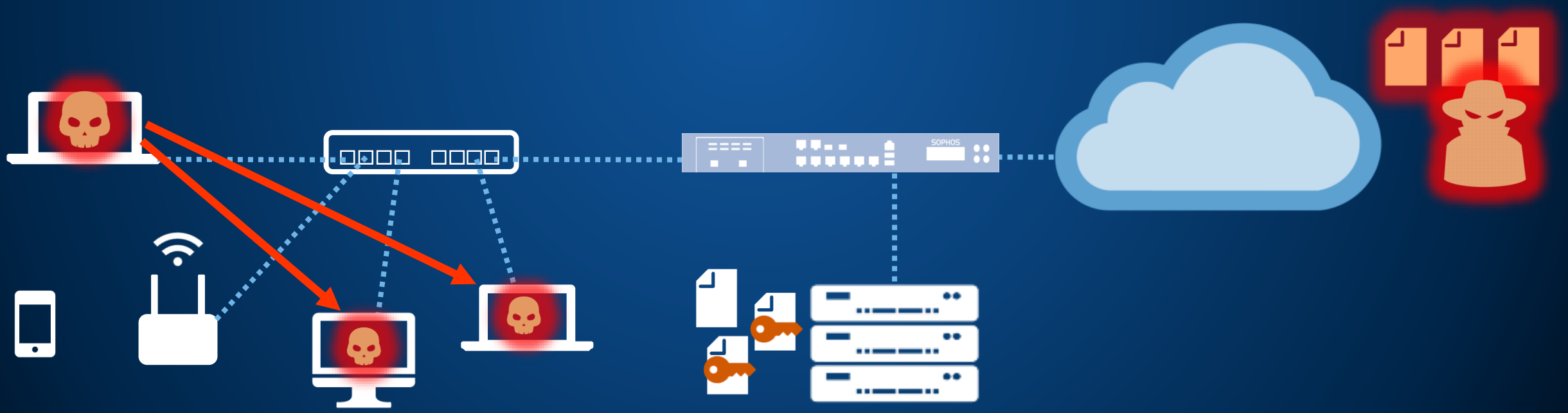


..und analysiert

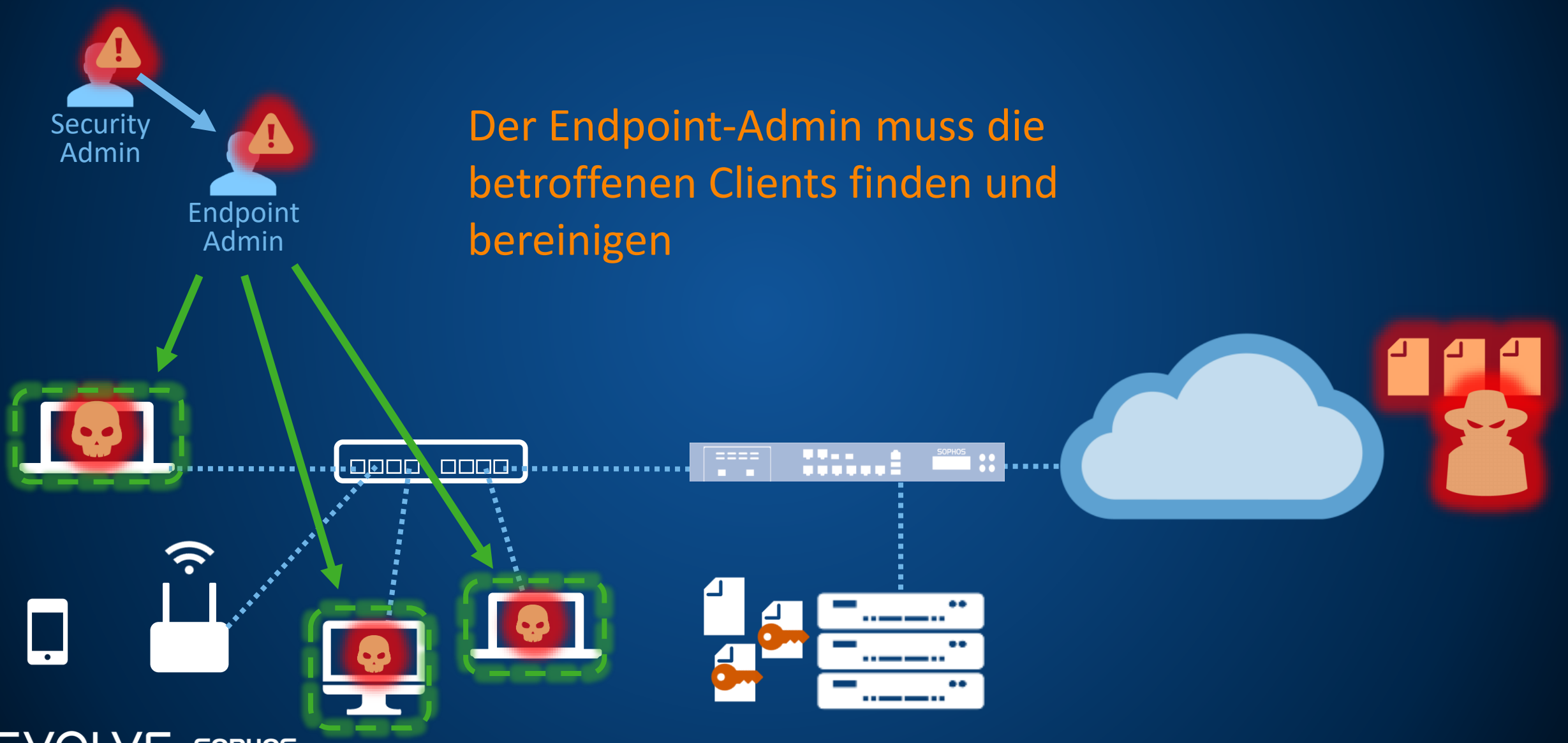


Security Admin

..außerdem wurden weitere Endpoints infiziert

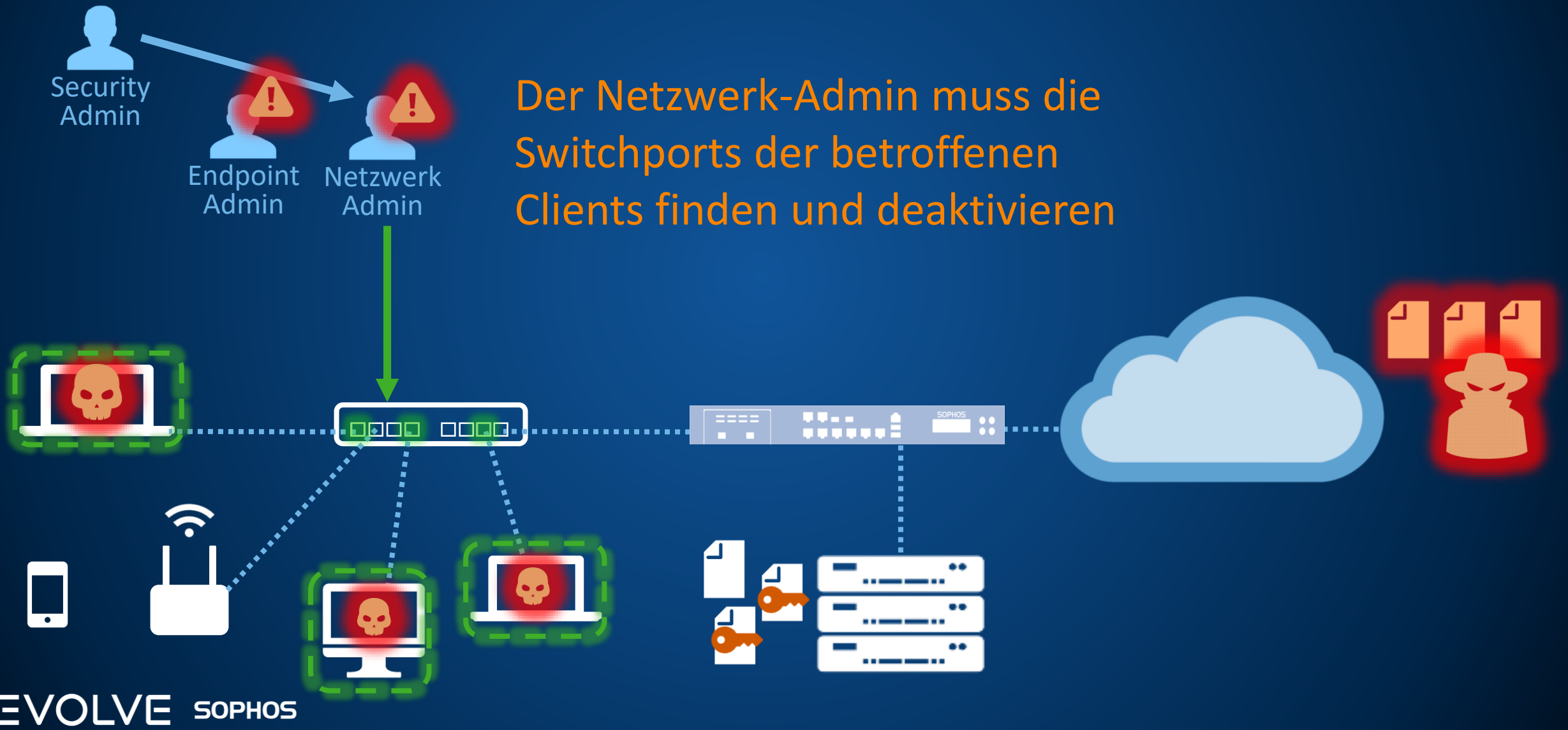


Action!!!

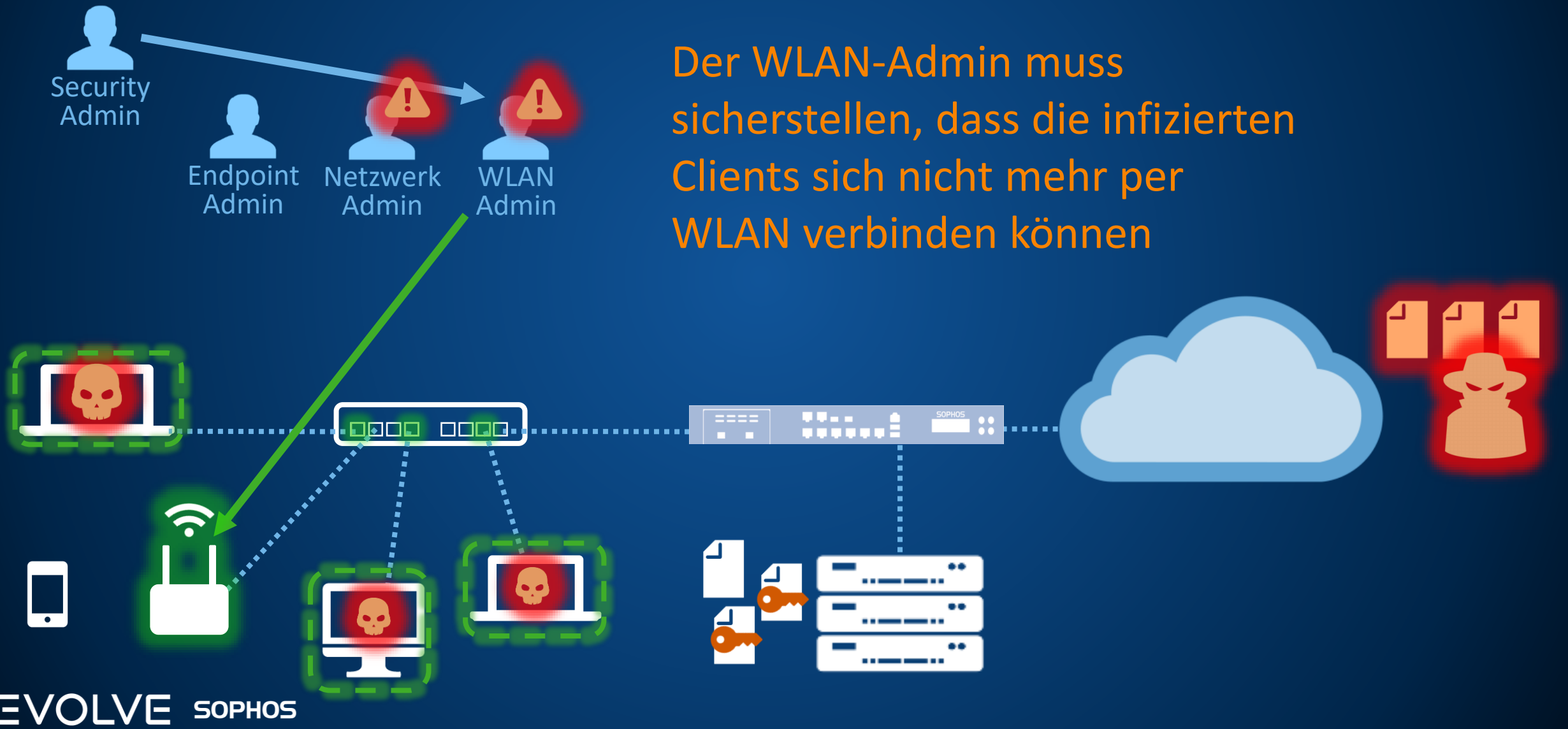


Der Endpoint-Admin muss die betroffenen Clients finden und bereinigen

Action!!!

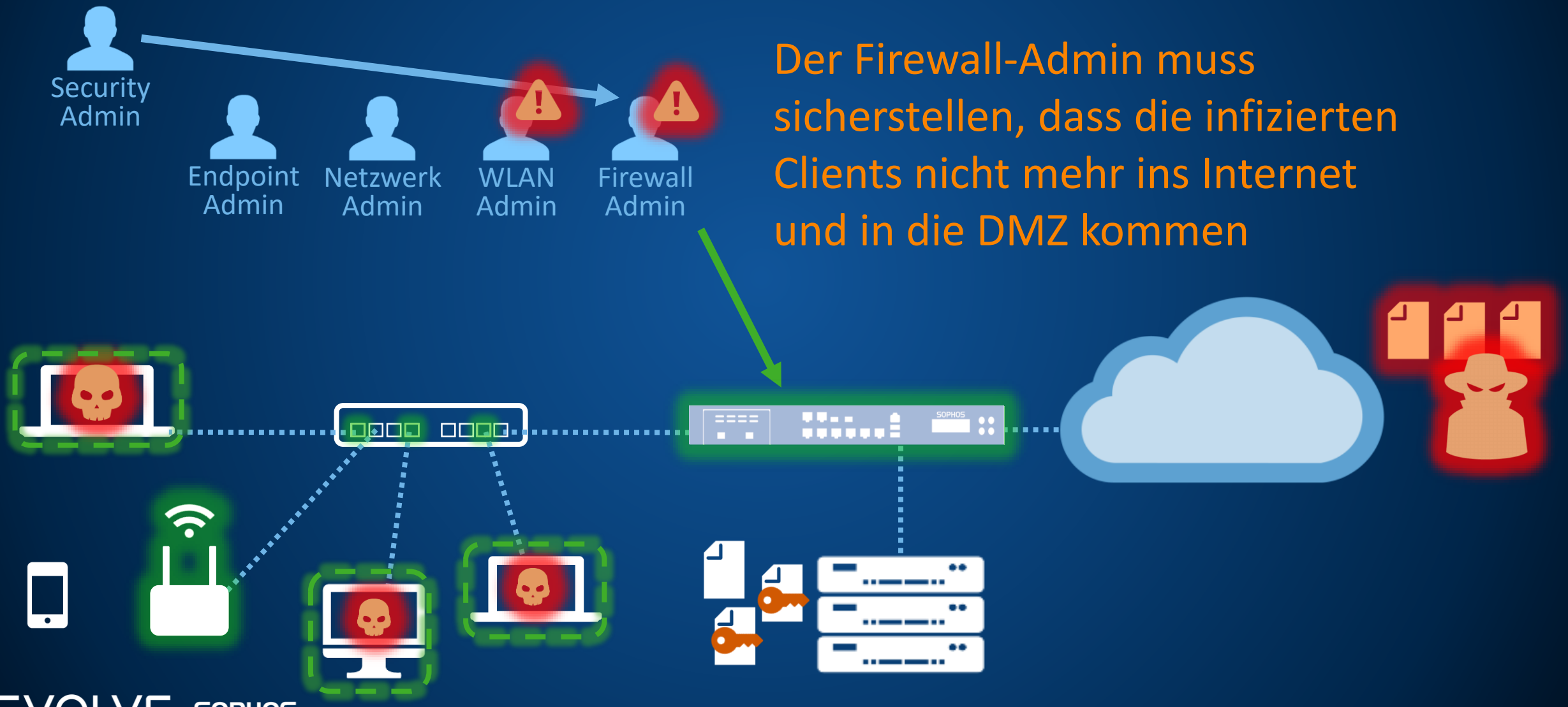

Security Admin
Endpoint Admin
Netzwerk Admin
Der Netzwerk-Admin muss die Switchports der betroffenen Clients finden und deaktivieren
SOPHOS

Action!!!



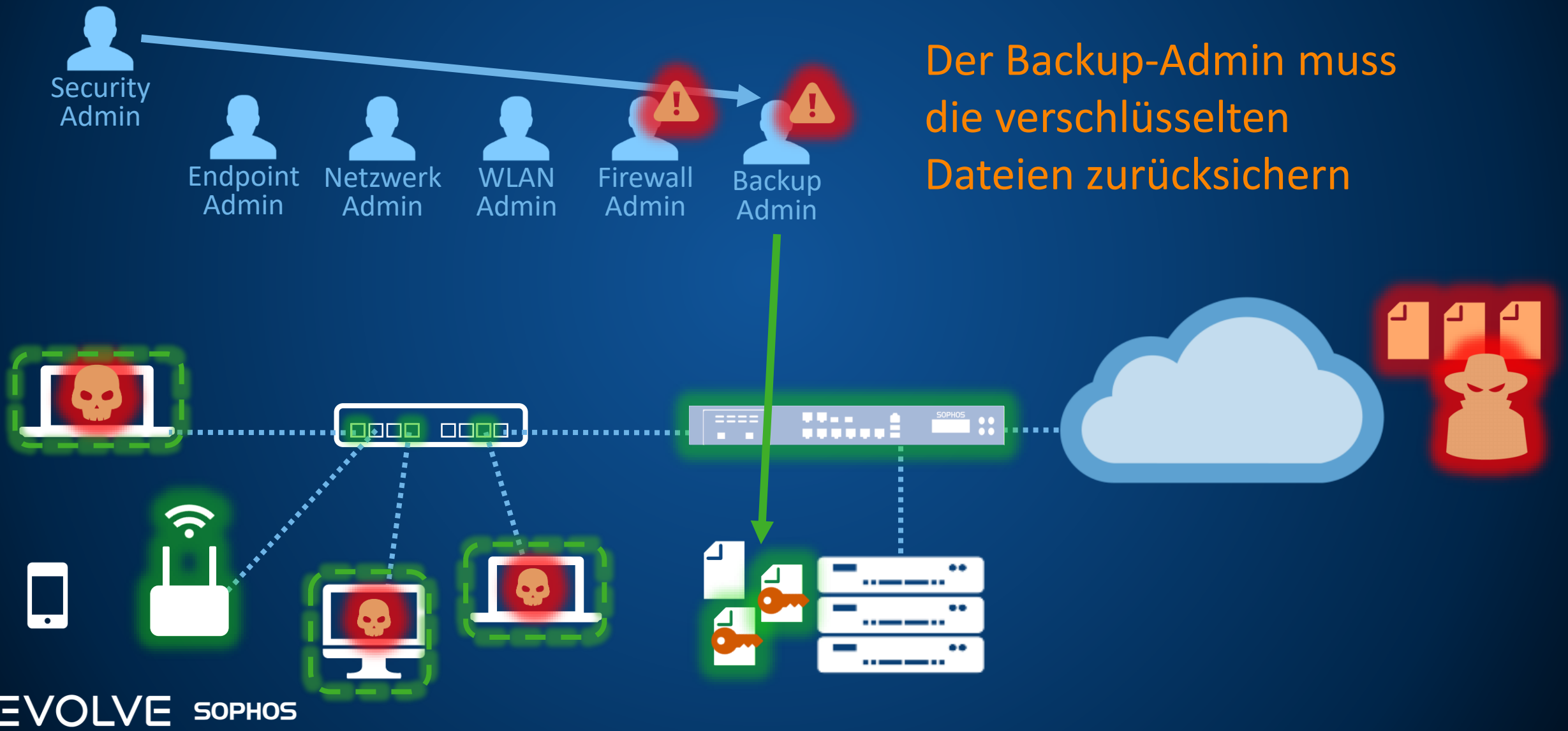
Der WLAN-Admin muss sicherstellen, dass die infizierten Clients sich nicht mehr per WLAN verbinden können

Action!!!



Der Firewall-Admin muss sicherstellen, dass die infizierten Clients nicht mehr ins Internet und in die DMZ kommen

Action!!!


Security Admin
Endpoint Admin
Netzwerk Admin
WLAN Admin
Firewall Admin
Backup Admin
Der Backup-Admin muss die verschlüsselten Dateien zurücksichern
SOPHOS

Action!!!

Jetzt wird der CISO informiert..

Action!!!

Security Admin

Endpoint Admin

Netzwerk Admin

WLAN Admin

Firewall Admin

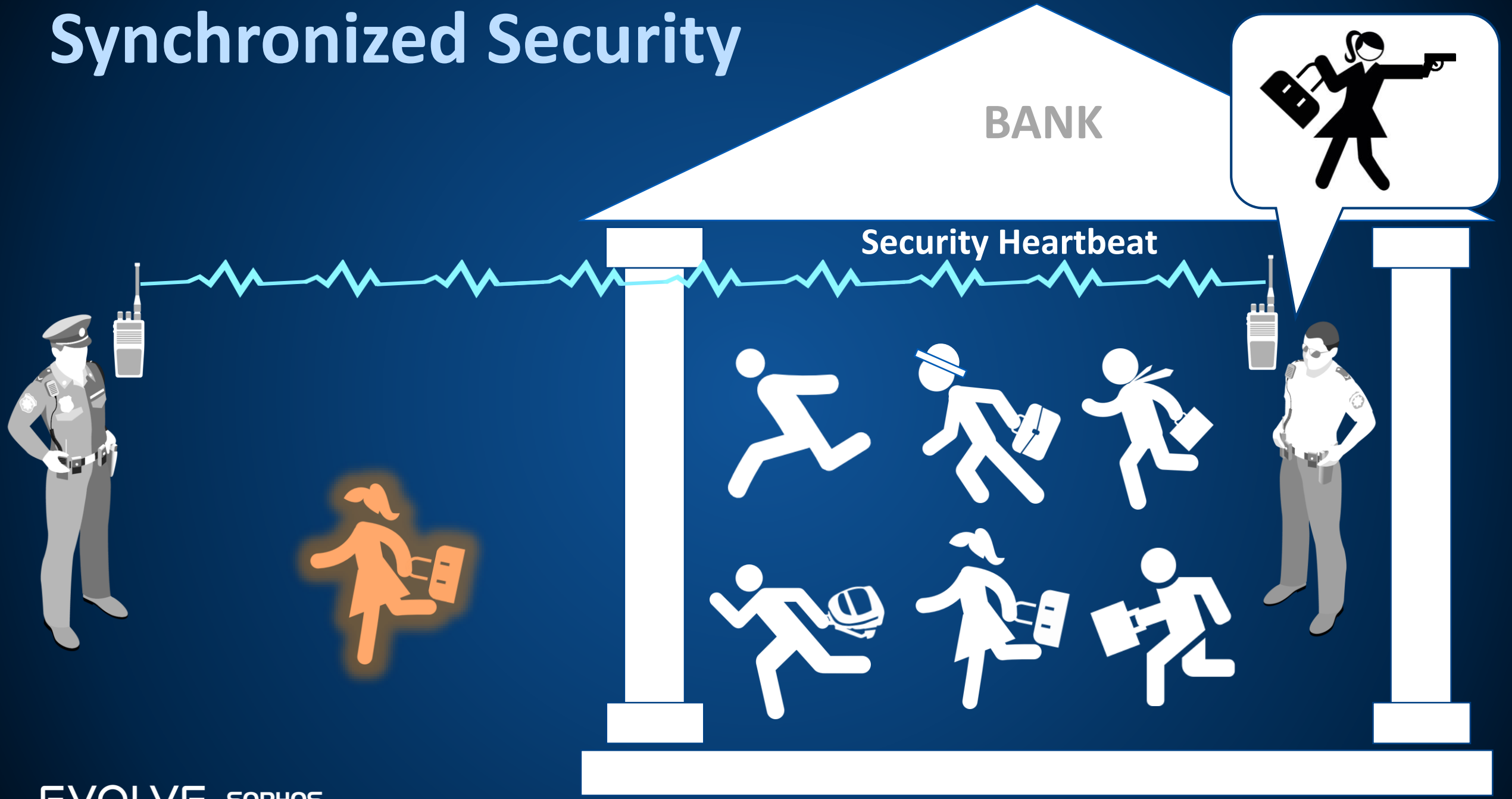
Backup Admin

CISO

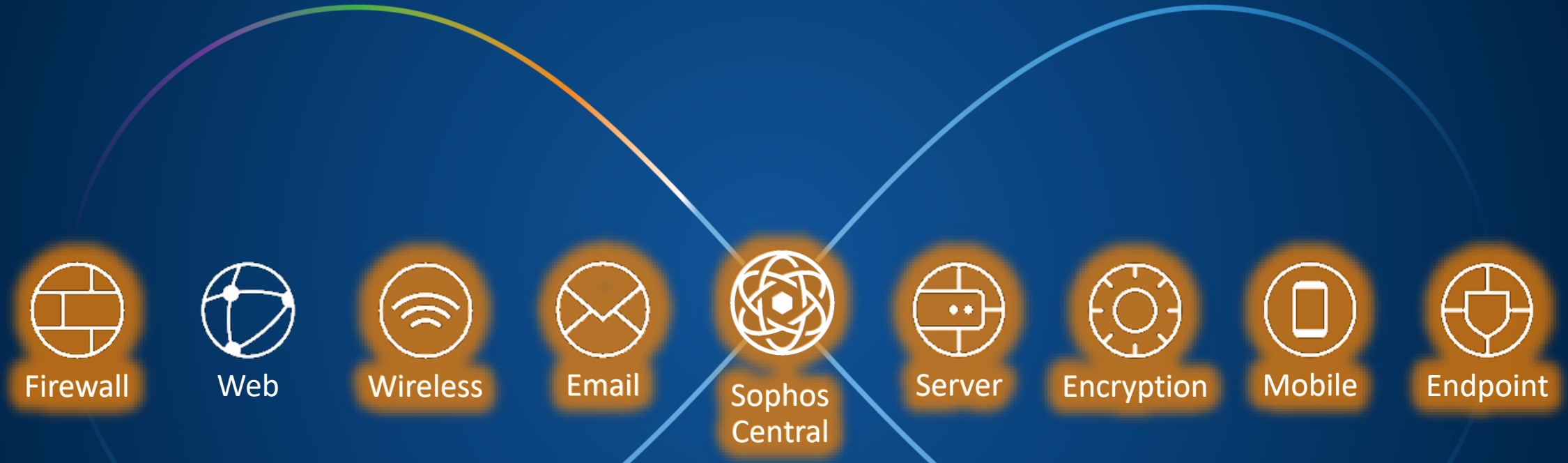
CEO

..der den CEO informiert,
dass Daten gestohlen wurden

Synchronized Security



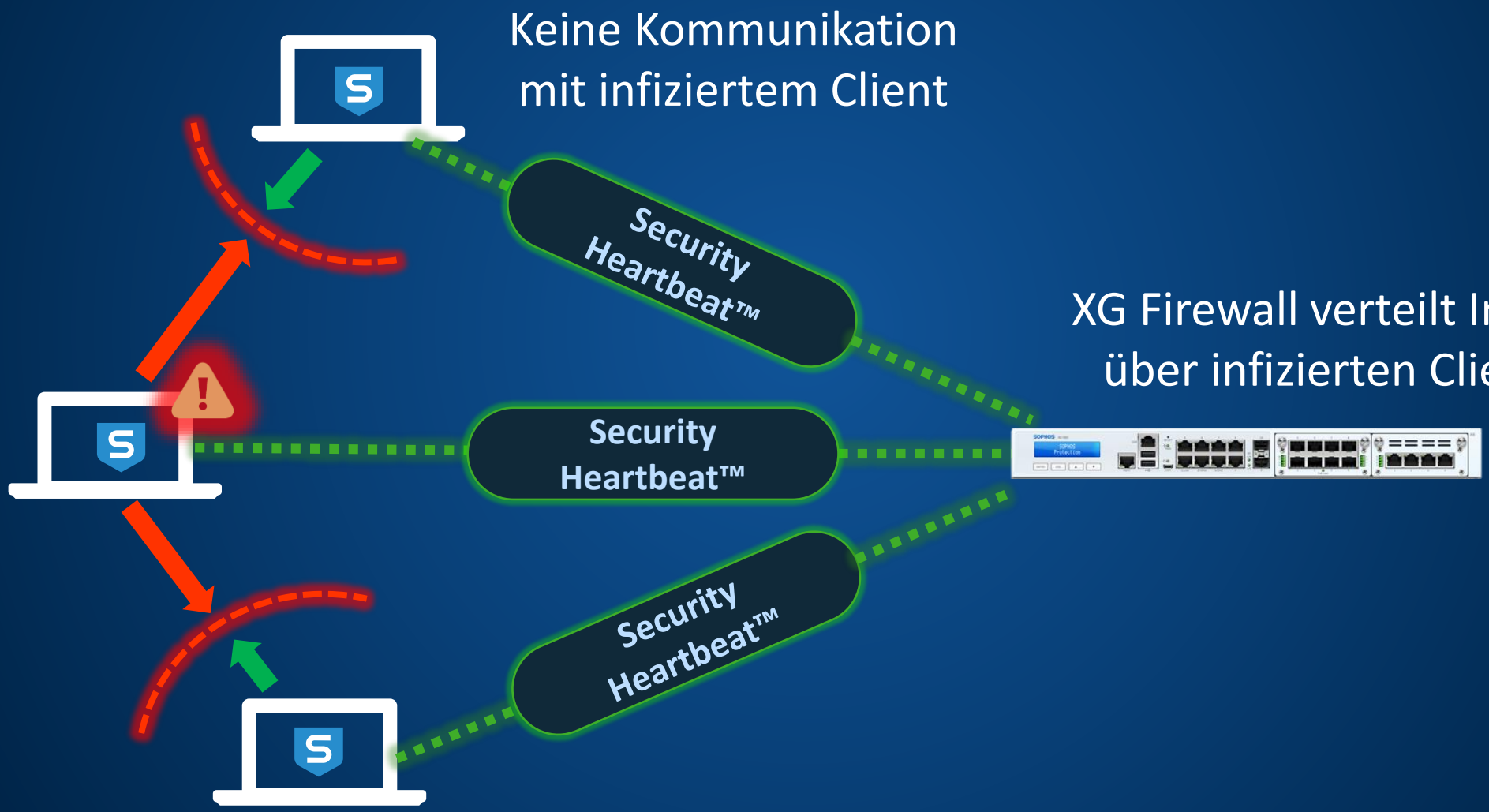
Sophos Synchronized Security



Automatisches Verhindern von Netzwerkverbindungen durch die XG Firewall

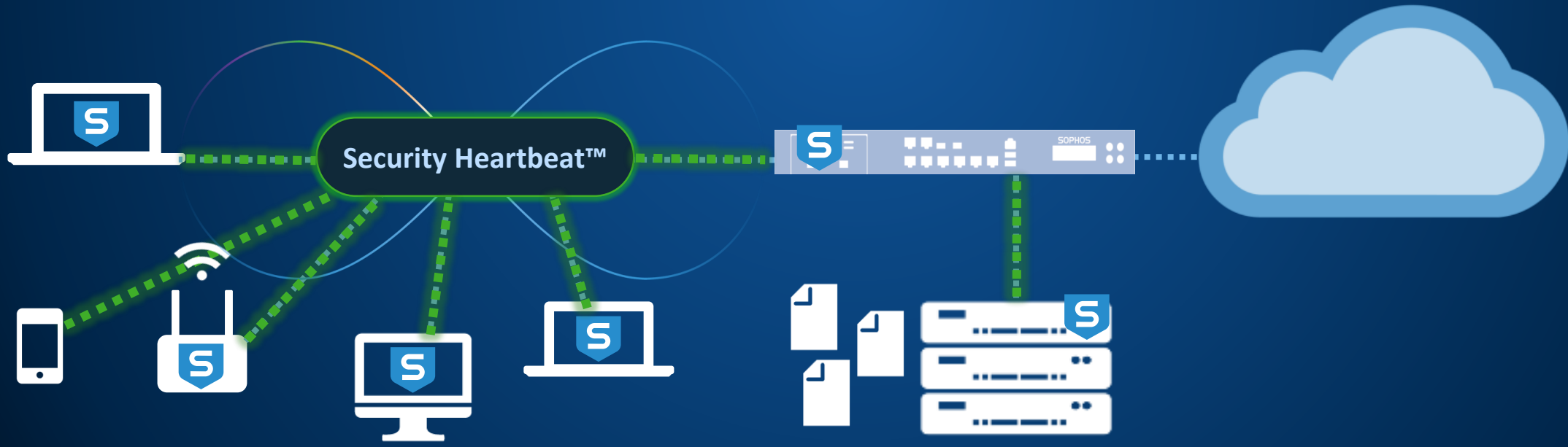
XG Firewall verhindert Verbindungen in separierte Netze

Lateral Movement Protection mit XG Firewall 17.5



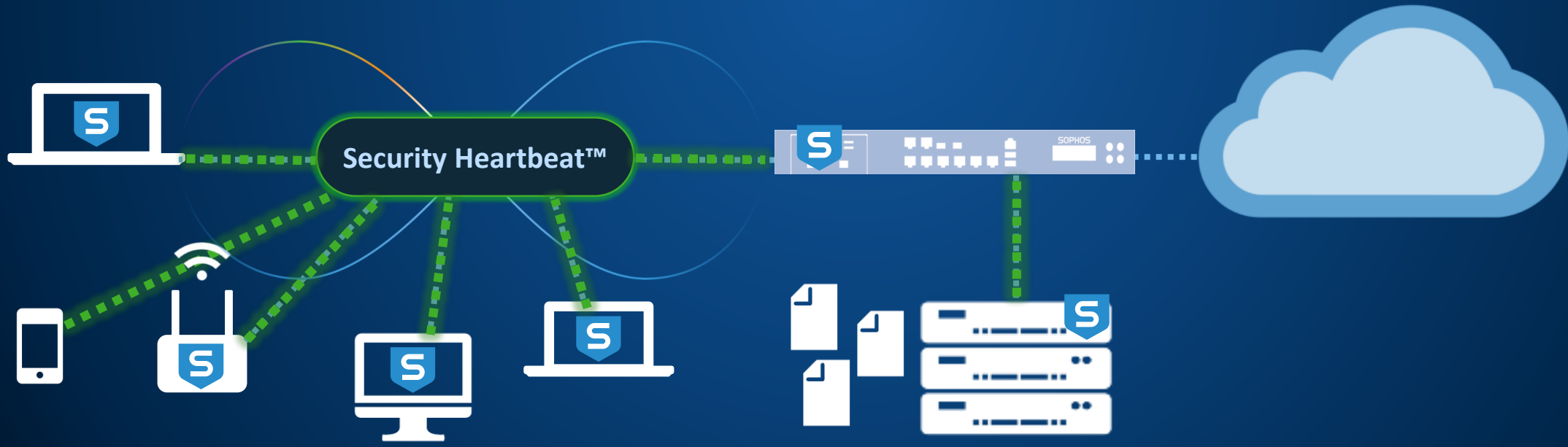
Und wie sieht es mit Synchronized Security aus?

Vorgehen bei Bedrohungen mit Synchronized Security



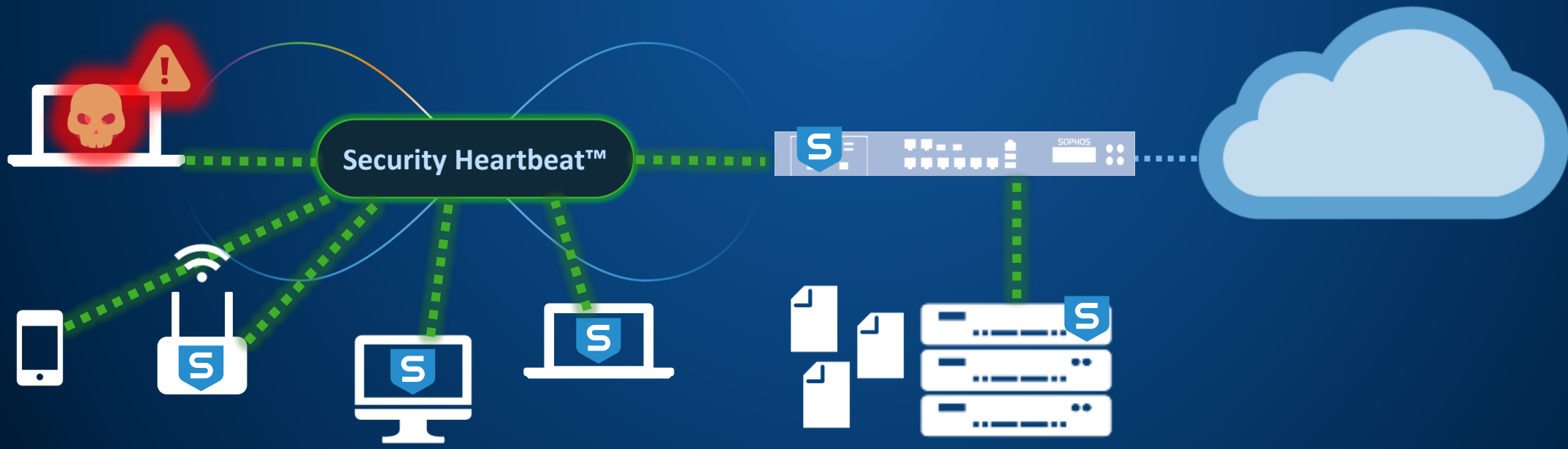
Vorgehen bei Bedrohungen mit Synchronized Security

Clients, Server, Mobilgeräte, WLAN-APs
und Firewall kommunizieren per
SecurityHeartbeat direkt miteinander



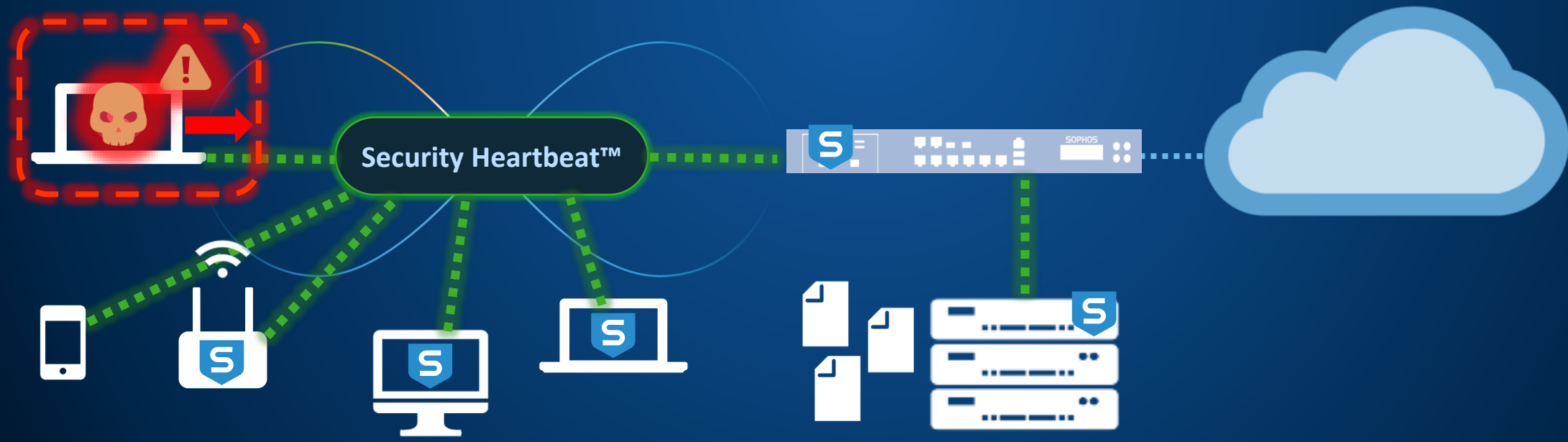
Vorgehen bei Bedrohungen mit Synchronized Security

Bei einer Bedrohung werden alle Komponenten informiert und reagieren automatisch



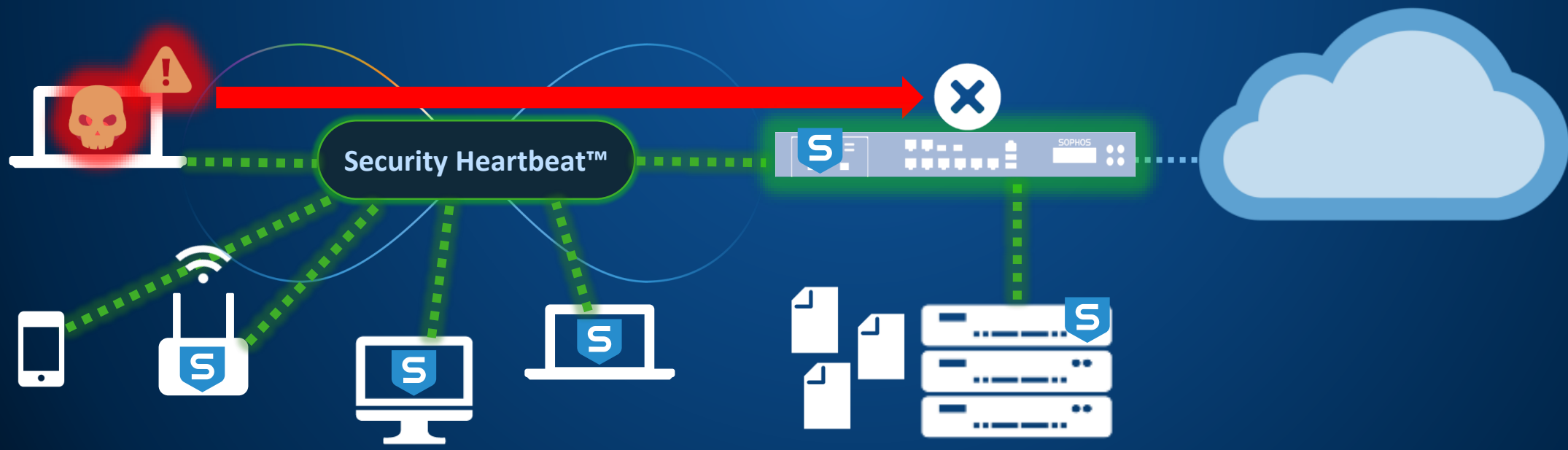
Vorgehen bei Bedrohungen mit Synchronized Security

Der Client isoliert sich selbst..



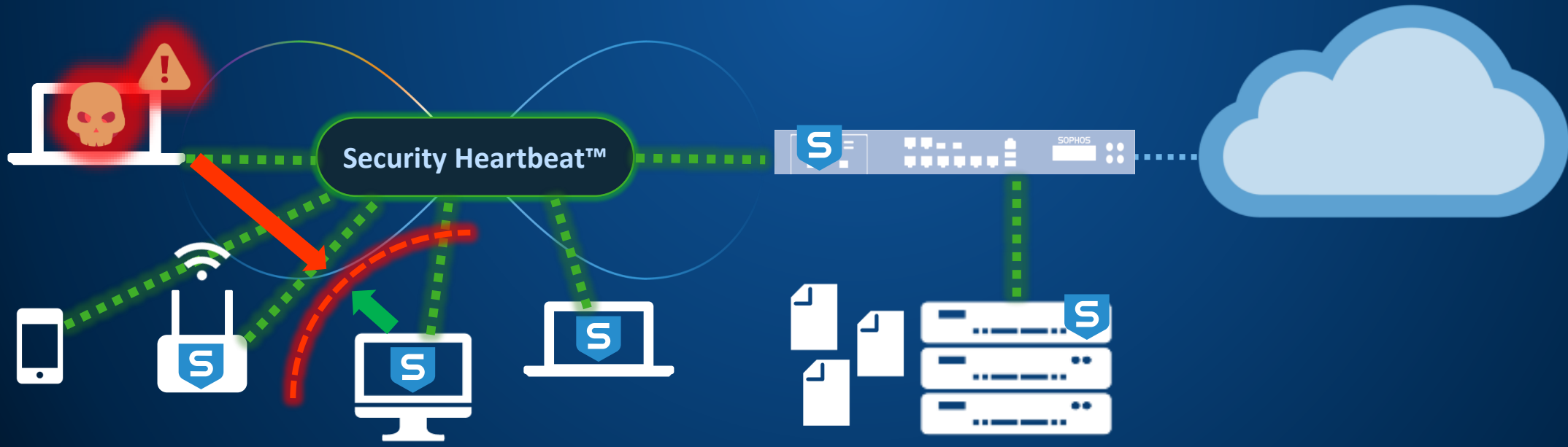
Vorgehen bei Bedrohungen mit Synchronized Security

Die Firewall nimmt den Client in Netzwerkquarantäne und verhindert Kommunikation ins Internet oder die DMZ



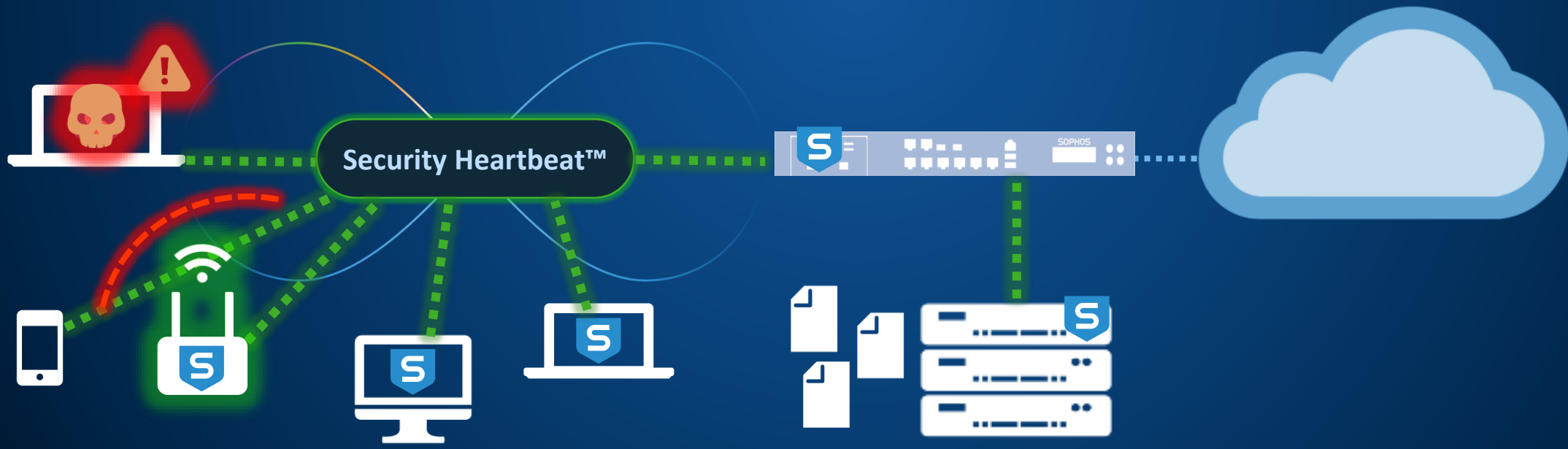
Vorgehen bei Bedrohungen mit Synchronized Security

Die Clients im selben Netz kommunizieren nicht mehr mit dem infizierten Client



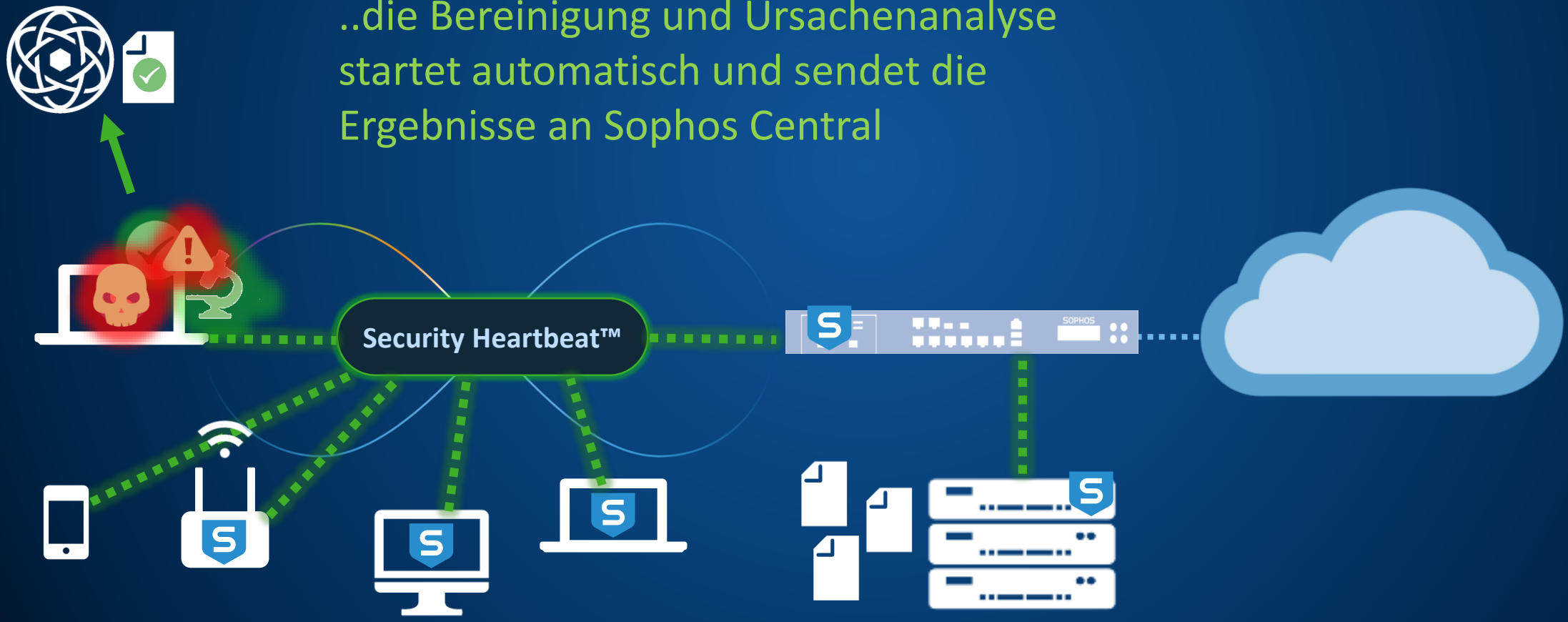
Vorgehen bei Bedrohungen mit Synchronized Security

Der WLAN Access Point lässt
den infizierten Client nicht
mehr ins interne WLAN



Vorgehen bei Bedrohungen mit Synchronized Security

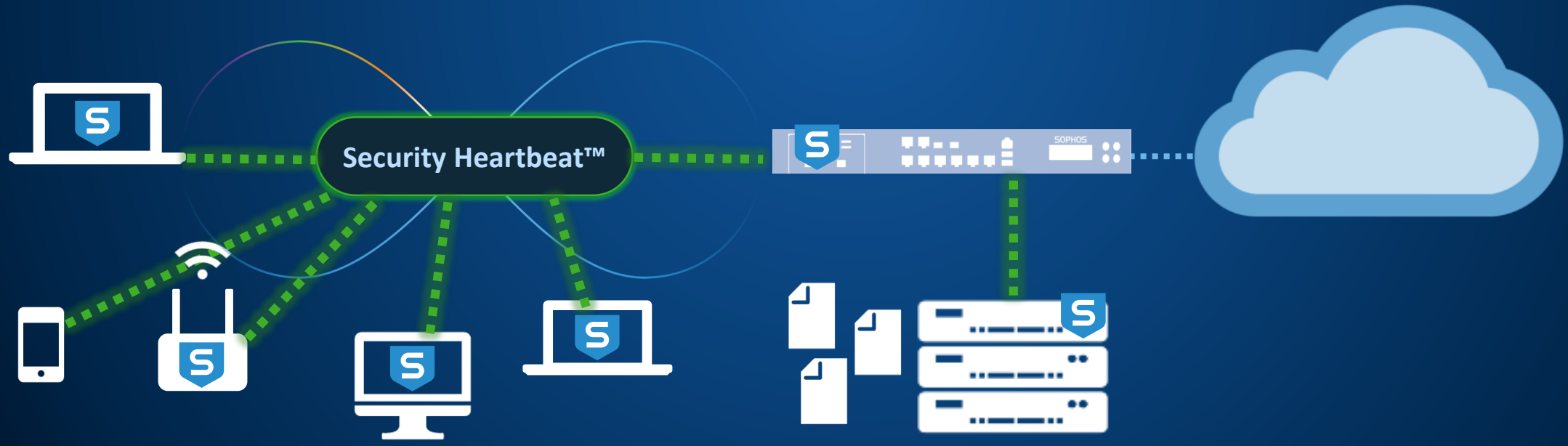
..die Bereinigung und Ursachenanalyse startet automatisch und sendet die Ergebnisse an Sophos Central



Vorgehen bei Bedrohungen mit Synchronized Security

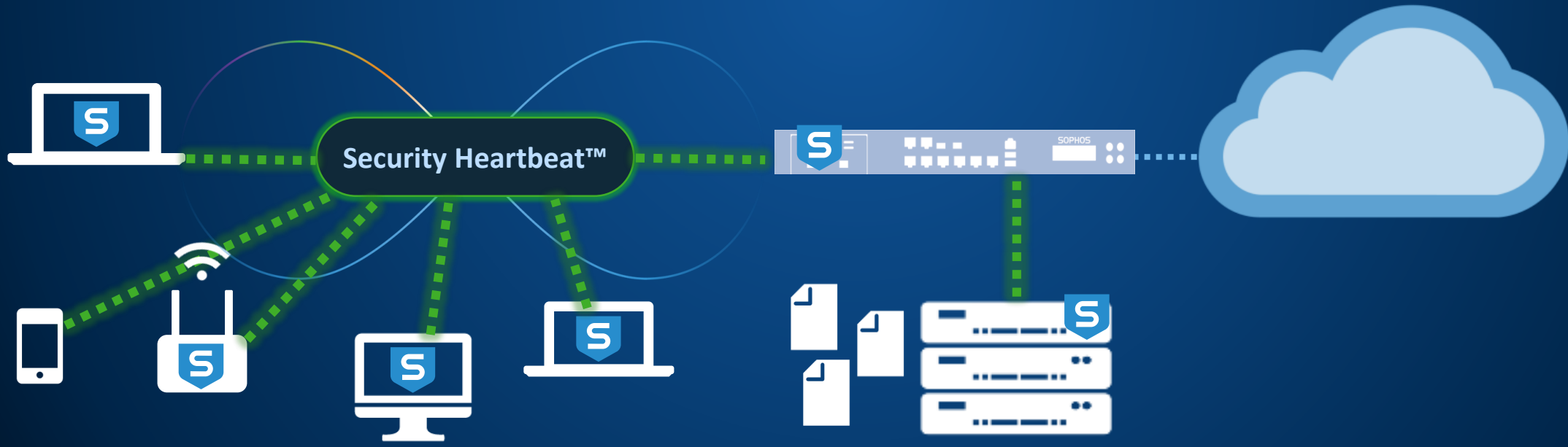
Admin

..der Admin erhält den Bericht, dass die Bedrohung automatisch eingedämmt wurde und keine Daten gestohlen wurden

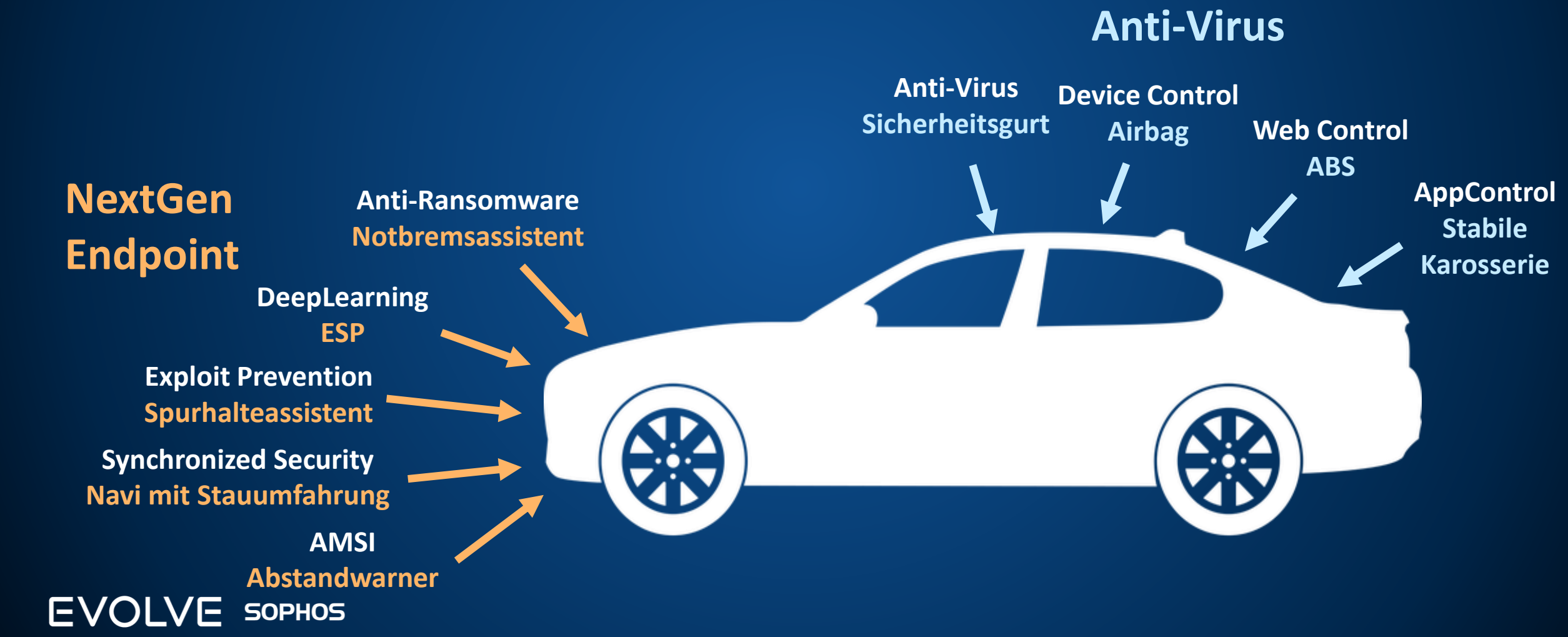


Vorgehen bei Bedrohungen mit Synchronized Security

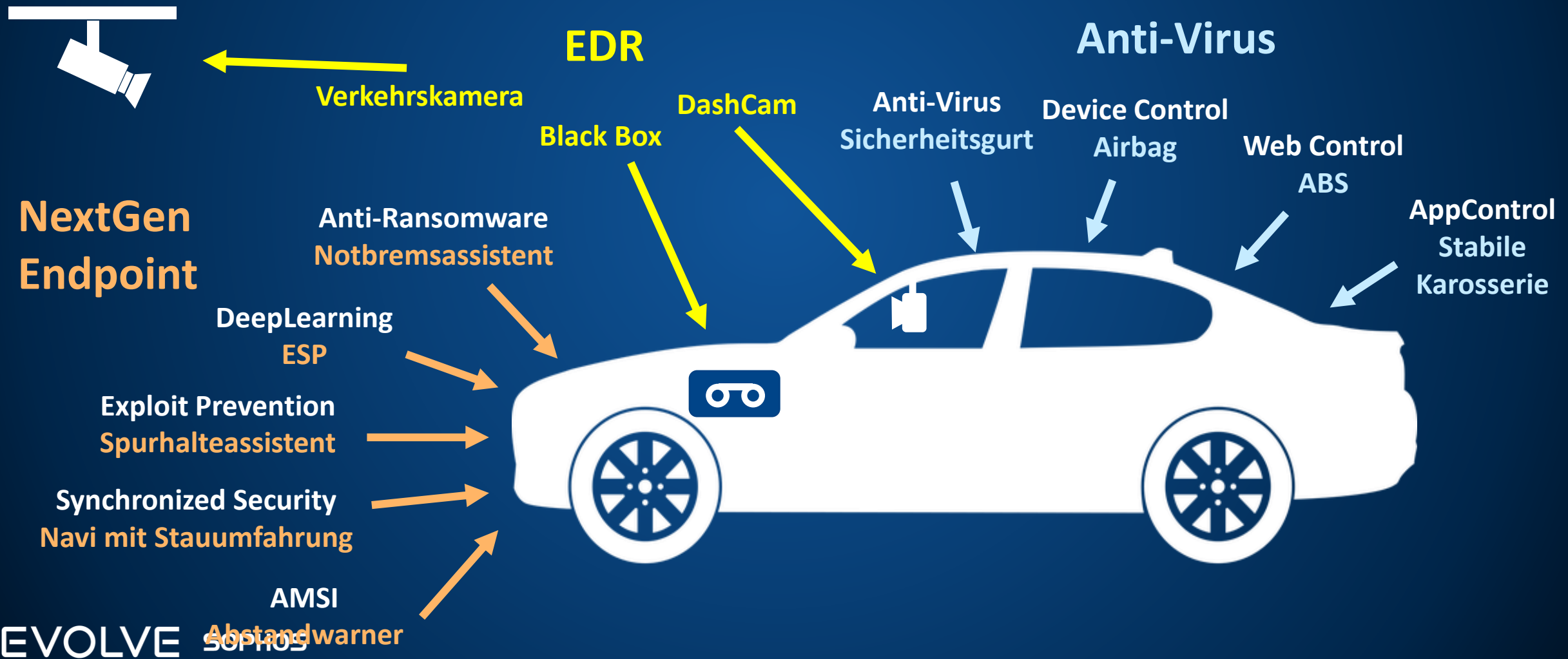
..und der CEO ist zufrieden, dass die IT Sicherheit einfach funktioniert.



Von AntiVirus zu NextGen



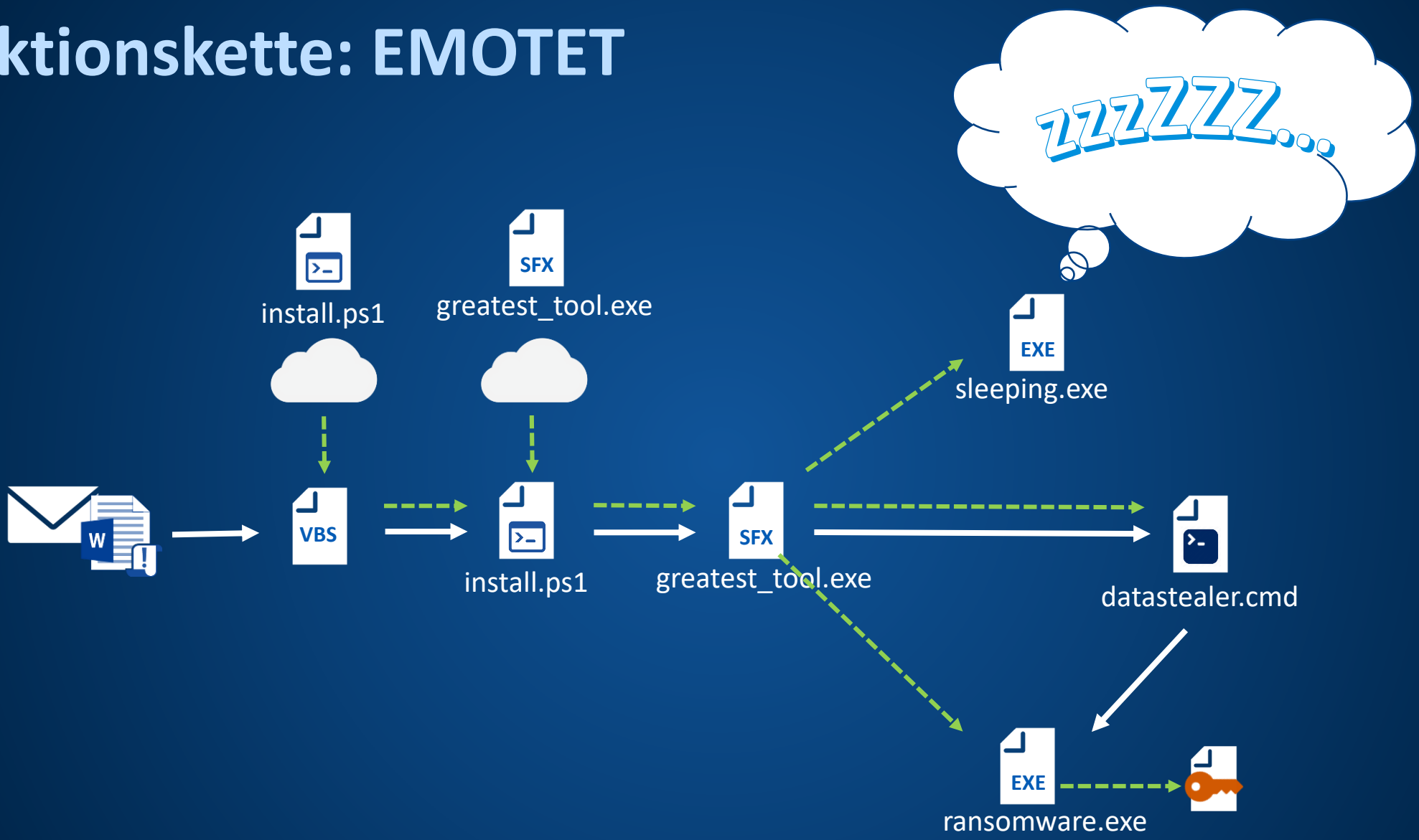
Von Anti-Virus zu NextGen und EDR



EDR

Endpoint Detection and Response

Infektionskette: EMOTET



Live Demo

SOPHOS CENTRAL Admin

Übersicht

- Dashboard
- Alarme
- Protokolle & Berichte
- Personen
- Geräte
- Globale Einstellungen
- Geräte schützen

MEINE PRODUKTE

- Endpoint Protection
- Server Protection
- Mobile
- Encryption
- Web Gateway
- Wireless
- Email Gateway
- Firewall-Verwaltung

Sophos Central Dashboard

Snapshot Ihrer Schutzmaßnahmen anzeigen

Hilfe · Michael Veit
Sophos Ltd · Superadmin

Letzte Alarme

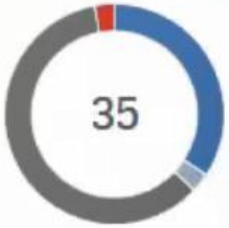
Alle Alarme anzeigen

!	10. Jan. 2019 11:05	Bösartiger Traffic erkannt: 'C2/Generic-B' at 'C:\users\admin\appdata\lo...	W10PROTECTED\admin	W10Protected
!	10. Jan. 2019 11:05	CryptoGuard hat Ransomware entdeckt in C:\Users\admin\AppData\Loc...	W10PROTECTED\admin	W10Protected

Geräte und Benutzer: Übersicht

Bericht anzeigen

Aktivitätsstatus Endpoint-Computer



- 12 Aktiv
- 1 Inaktiv 2+ Wochen
- 21 Inaktiv 2+ Monate
- 1 Nicht geschützt

Web-Statistiken

Berichte anzeigen

1 Web-Bedrohungen Blockiert	4 Richtlinienverstöße Blockiert
0 Richtlinien-Warnungen Ausgegeben	0 Richtlinien-Warnungen Fortgefahren

Übersicht über Web Gateway-Blockierungen

Bericht anzeigen

7 T | 14 T | 30 T

0
Insgesamt blockiert

Keine Blockiermaßnahmen gemeldet.
Aktualisieren Sie Ihre Web Gateway-

Email Security

Bericht anzeigen

Eingehend | Ausgehend

15 Gescannte E-Mails
16 Gescannte Posteingänge

- 0 Spam
- 0 Komplexe Bedrohungen
- 0 Viren
- 0 Authentifizierungsfehler

Endpoint Protection - Dashboard

Überblick / Endpoint Protection Dashboard

Hilfe ▾ Michael Veit ▾
Sophos Ltd - Superadmin

Jüngste Bedrohungsfälle

Alle Bedrohungsfälle anzeigen

Von Sophos erzeugt | Vom Admin erzeugt

Erstellt um	Priorität	Name	Benutzer	Gerät
10. Jan. 2019 11:39	Hoch	C2/Generic-B	W10PROTECTED\admin	W10Protected
10. Jan. 2019 11:34	Hoch	CryptoGuard	W10PROTECTED\admin	W10Protected
10. Jan. 2019 11:19	Hoch	C2/Generic-B	W10PROTECTED\admin	W10Protected
10. Jan. 2019 11:14	Hoch	CryptoGuard	W10PROTECTED\admin	W10Protected
10. Jan. 2019 09:35	Hoch	C2/Generic-B	W10PROTECTED\admin	W10Protected

Endpoint Protection - CryptoGuard

W10Protected	Hauptursache	Beacon	Erkannt	Bereinigt
172.16.1.20	Outlook	ransomware.exe	10. Jan. 2019 11:27	

Übersicht

Name der Erkennung:	CryptoGuard
Grundursache:	outlook.exe
Mögliche involvierte Daten:	12 Geschäftsdateien
Wo:	Unter W10Protected Für W10PROTECTED\admin
Wann:	Erkannt am 10. Jan. 2019 11:27

Empfohlene nächste Schritte

Einen Status für den Bedrohungsfall setzen — Priorität: Hoch — Status: Neu

3 Prozesse untersuchen, die wir mit der Reputation "unsicher" markiert haben.
Siehe die untenstehende Grafik für weitere Details

Diesen Computer isolieren während Sie untersuchen

Computer scannen

Analysieren | Falldatensatz

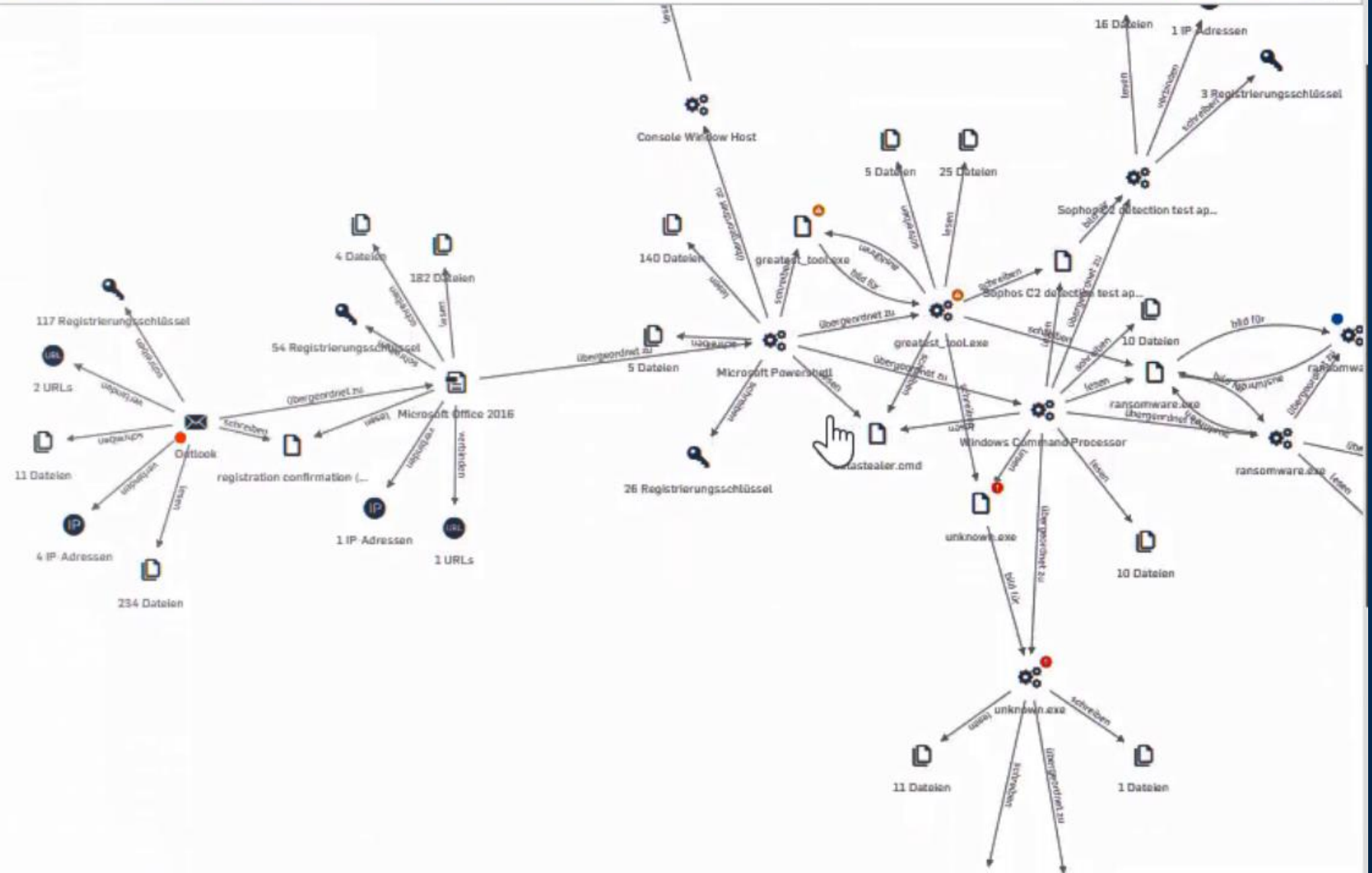
Filter: Prozesse | Andere Dateien | Geschäftsdateien | Netzwerkverbindungen | Registrierungsschlüssel — Vollständiges Diagramm a

Wann: Erkannt am 15. Jan. 2019 10:54

Analysieren | Falldatensatz

Filter: Prozesse | Andere Dateien | Geschäftsdateien | Netzwerkverbindungen | Registrierungsschlüssel

Vollständiges Diagramm an



SOPHOS CENTRAL Admin

Endpoint Protection

Zurück zur Übersicht

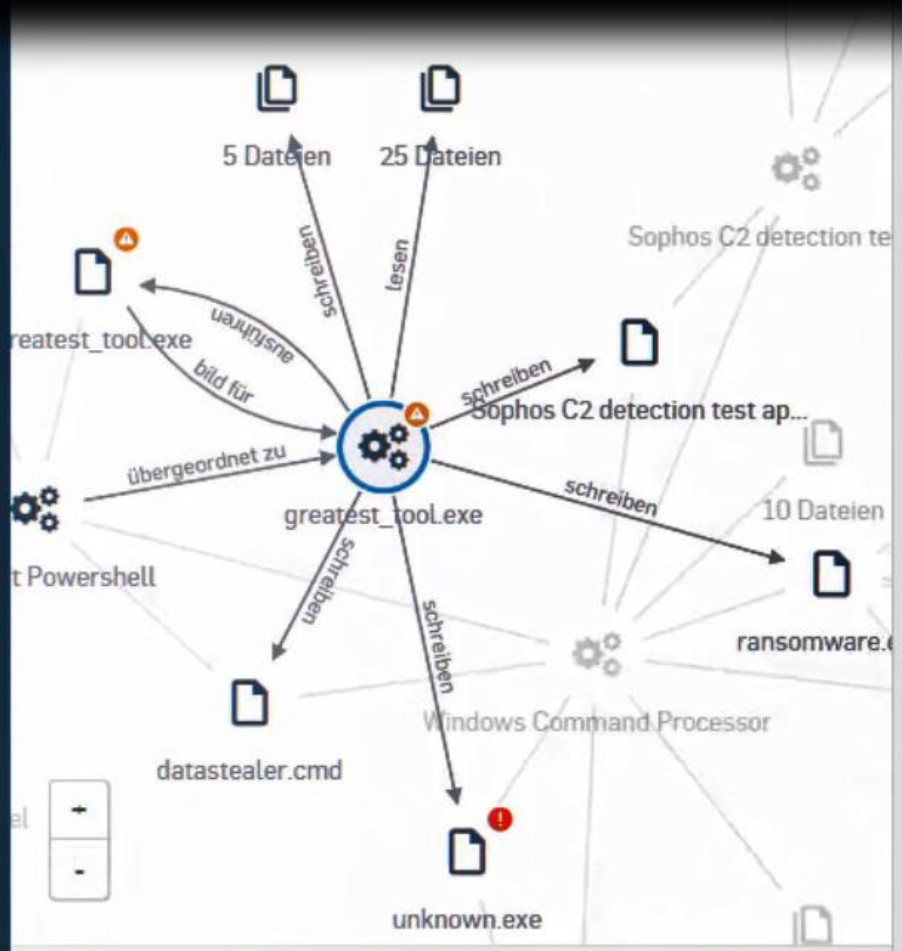
ANALYSIEREN
- Dashboard
- Protokolle & Berichte

ERKENNUNG UND BESEITIGUNG
- Bedrohungsfälle
- Suchen nach Bedrohungen

SCHUTZ VERWALTEN
- Personen
- Computer

KONFIGURIEREN
- Richtlinien
- Einstellungen
- Geräte schützen

SOPHOS CENTRAL
- Kostenlose Testversionen



Hauptursache | Beacon | Unsichere Reputation | Schlecht

Suchen

Name	Typ
callhome.exe	Prozess
ransomware.exe	Prozess
conhost.exe	Prozess

Prozessdaten : greatest_tool.exe

Prozessdaten | Zusammenfassung des Berichts | Analyse des maschinellen Lernens | Datei-Eigenschaften | Dateiaufschlüsselung

Reputation zum Zeitpunkt der Erstellung des Falles: **Unsichere Reputation**

Bekannter schlechter Ruf — Bekannter guter Ruf

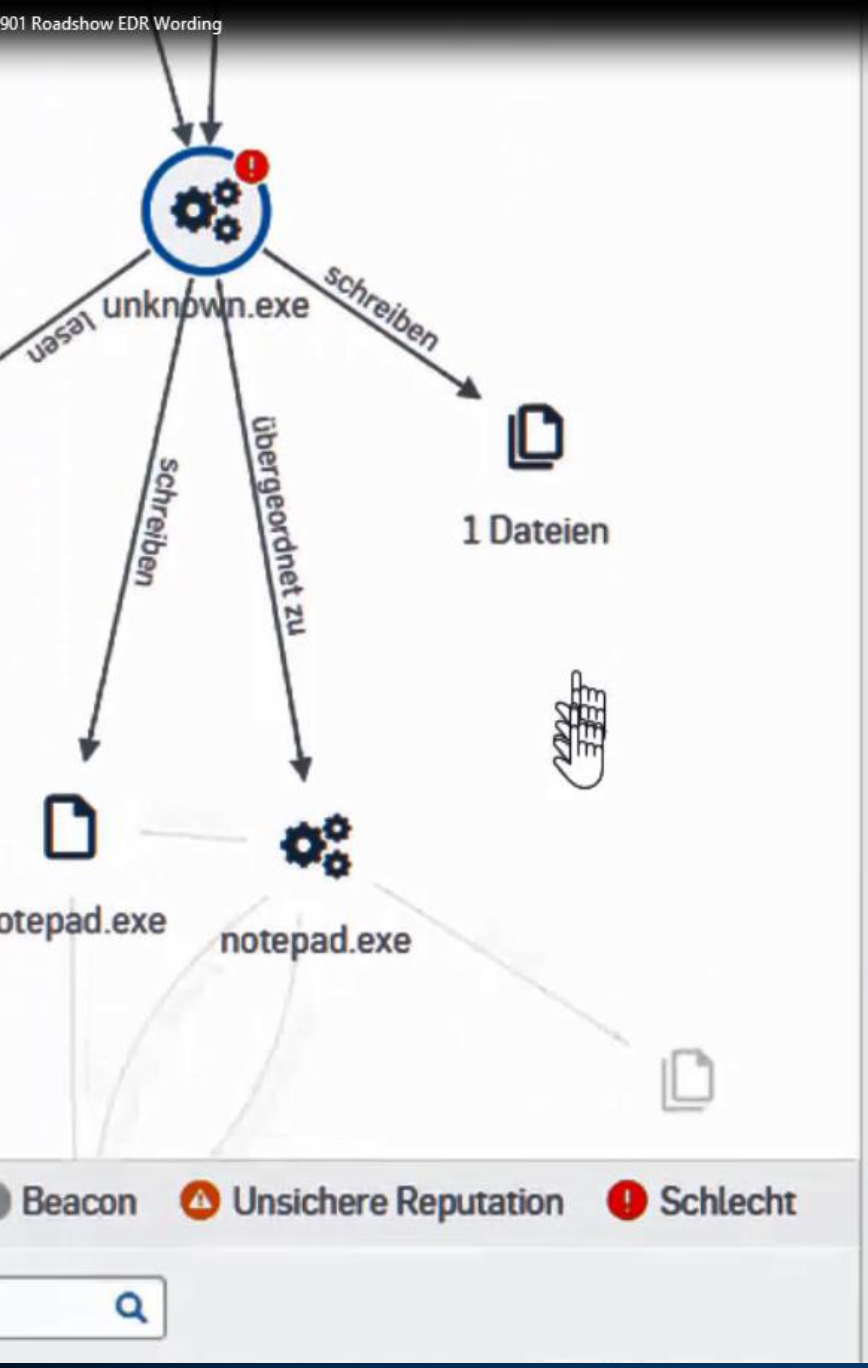
SOPHOSLABS Bedrohungsdaten

Aktueller Bericht erstellt: 10. Jan. 2019 09:51

Aktuellste Daten anfordern

Hinweis: Wenn Sie die neuesten Informationen abrufen möchten, werden Ihre Dateien zur weiteren Analyse an Sophos gesendet. Mehr erfahren

Pfad:	c:\users\admin\appdata\local\temp\greatest_tool.exe
Name:	greatest_tool.exe
Befehlszeile:	"C:\Users\admin\AppData\Local\Temp\greatest_tool.exe" -y -pmypass
Prozess-ID:	780
Prozess ausgeführt von:	W10PROTECTED\admin
SHA256:	9f463e6a0e66b09d7260774b039ede5ec364b6bd37ad03c3249eee10303f57fd
Startzeit:	15. Jan. 2019 10:54
Endzeit:	15. Jan. 2019 10:54
Dauer:	767ms
Bezüglich dieses Artefakts ausgeführte Aktionen:	Keiner
Von diesem Artefakt	



Prozessdaten | Zusammenfassung des Berichts | Analyse des maschinellen Lernens | Datei-Eigenschaften | Dateiaufschlüsselung

SOPHOSLABS Bedrohungsdaten

Aktueller Bericht erstellt: 15. Jan. 2019 13:33

Attribute : 69% Verdächtig

Über 29 Million bekannte gute und über 15 Million bekannte schädliche Elemente wurden analysiert.

Attribute	Gesehen in: Bekannte schädliche Dateien	Bekannte gute Dateien
Code injection capabilities: "OpenProcess"	25.1k	25.4k
Code injection capabilities: "WriteProcessMemory"	23.9k	23.3k
Has Internet access capabilities: "InternetCloseHandle"	50.8k	46.4k
Has Internet access capabilities: "InternetReadFile"	46.6k	40.6k
Code injection capabilities: "VirtualAllocEx"	19.3k	8.4k

Code-Ähnlichkeit : 35% Verdächtig

SOPHOS CENTRAL
Admin

Endpoint Protection

Zurück zur Übersicht

ANALYSIEREN
Dashboard
Protokolle & Berichte

ERKENNUNG UND BESEITIGUNG
Bedrohungsfälle
Suchen nach Bedrohungen

SCHUTZ VERWALTEN
Personen
Computer

KONFIGURIEREN
Richtlinien
Einstellungen
Geräte schützen

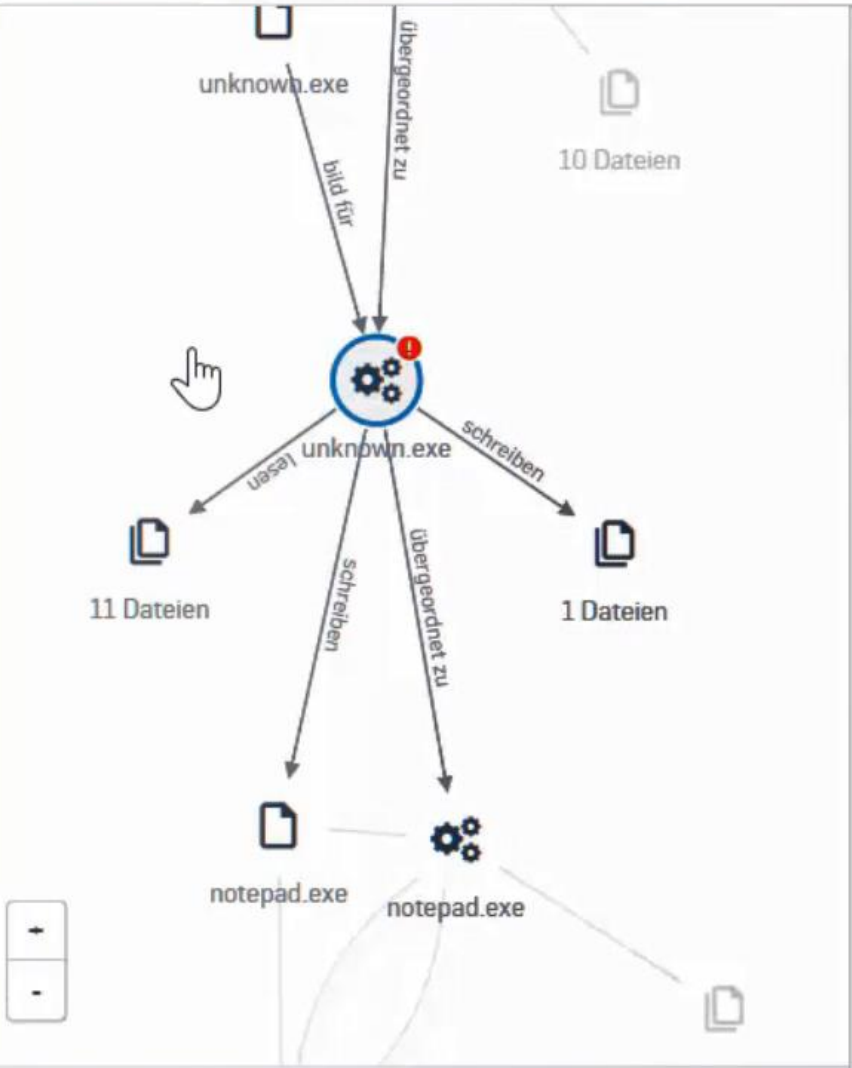
SOPHOS CENTRAL
Kostenlose Testversionen

Wann: Erkannt am 15. Jan. 2019 10:54

Analysieren | Falldatensatz

Filter: Prozesse | Andere Dateien | Geschäftsdateien | Netzwerkverbindungen | Registrierungsschlüssel

Vollständiges Diagramm a



PDF herunterladen | Nach Element suchen | Element blockiert

Was macht das?

Prozessdaten : unknown.exe

Prozessdaten | Zusammenfassung des Berichts | Analyse des maschinellen Lernens | Datei-Eigenschaften | Dateiaufschlüsselung

SOPHOSLABS Bedrohungsdaten

Aktueller Bericht erstellt: 15. Jan. 2019 13:33

Attribute : 69% Verdächtig

Über 29 Million bekannte gute und über 15 Million bekannte schädliche Elemente wurden analysiert.

Attribute	Gesehen in: Bekannte schädliche Dateien	Bekannte gute Dateien
Code injection capabilities: "OpenProcess"	25.1k	25.4k
Code injection capabilities: "WriteProcessMemory"	23.9k	23.3k
Has Internet access capabilities: "InternetCloseHandle"	50.8k	46.4k
Has Internet access capabilities: "InternetReadFile"	46.6k	40.6k
Code injection capabilities: "VirtualAllocEx"	19.3k	8.4k

Apropos MSP: EDR als MDR

EDR

Endpoint Detection and Response

SOFTWARE

MDR

Managed Detection and Response

SERVICE

Ab sofort verfügbar!

Expert-Led Threat Response

Managed Threat Response (MTR)

- Andere hören bei Benachrichtigung auf. Wir fangen da erst an.
- 24/7 threat hunting, detection, and response wird Ihnen von einem Expertenteam als full-managed service geboten.

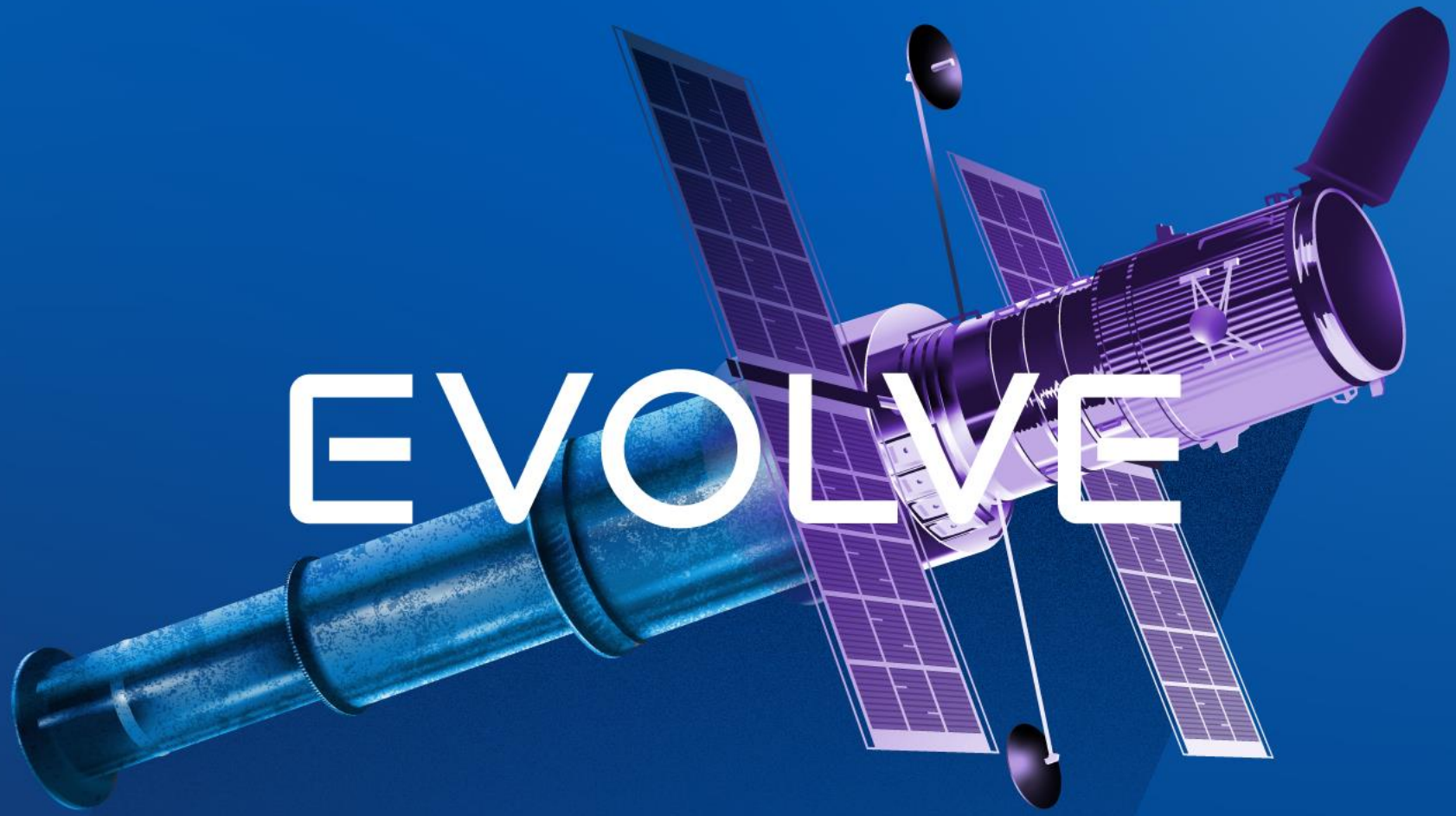
Analyst-Led Threat Hunting and Response

Targeted Actions to Neutralize Threats

Complete Transparency and Control

Wie unterscheiden sich die Endpoint Angebote?

CEP	CIXA	CIXAEDR	CIXAMTR
Basis Endpoint	NextGen Endpoint	NextGen Endpoint	NextGen Endpoint
Bekannte Malware	+ Zero Day / Ransomware	+ Hacker Aktivität	+ neue Angriffsszenarien
Signaturen/Heuristik	+ Deep Learning + Anti-Exploit + CryptoGuard	+ Bedrohungsindikatoren mit Machine Learning	+ menschliche und künstliche Intelligenz
Alarm/Report	Ursachenanalyse	Forensische Analyse + Bedrohungssuche	+ Zusammenfassung durch Analysten
IT des Kunden / MSP	IT des Kunden / MSP	IT des Kunden / MSSP	Sophos / MSSP



EVOLVE

SOPHOS

ROADSHOW 2019